Facultad de Ingeniería

Trabajo de Investigación

“Análisis, diseño e implementación de un sistema de encriptación de datos utilizando el método de la regleta”

Autor: Jennyfer Ivette Escudero Quintana – 1510762

Para obtener el Grado de Bachiller en:

Ingeniería de Sistemas e Informática

Lima, Julio 2019

RESUMEN

La empresa Deutsche Pharma suele compartir información confidencial entre sus trabajadores por la red, que, al ser vulnerada, perjudicaría a la empresa. Por tal motivo requiere un sistema seguro que encripte la información.

El objetivo de la presente investigación es realizar el análisis, diseño e implementación de un sistema de escritorio que permita encriptar la información que se comparte en la red, con el fin de protegerla. Se utilizó para el cifrado el método de la regleta, con una palabra clave y números claves para reforzar el algoritmo criptográfico.

La metodología empleada para el desarrollo del proyecto en esta investigación es SCRUM, se caracteriza por ser ágil para la gestión de proyectos. De acuerdo con esta metodología se identificó el equipo SCRUM y las tareas de las Historias de usuario a trabajar.

Finalmente, como resultado de la implementación se obtuvo un sistema con un cifrado seguro, que es amigable para los usuarios de la empresa. El sistema es portable y puede ser utilizado desde cualquier lugar, no se requiere de internet para utilizarlo. Se puede concluir que un algoritmo criptográfico es más seguro cuando es personalizado.

Dedicatoria

A Dios, quien sostiene mi vida en sus manos y es mi esperanza. A mi familia y a mi novio, quienes me apoyan y animan.

Agradecimiento

A Dios, sin él no hubiese podido lograrlo, todo lo que tengo es por su gracia y misericordia.

A mi familia y a mi novio, quienes me han apoyado en todo momento.

A los profesores quienes me enseñaron lo aprendido para ejercer mi profesión.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En el presente Trabajo de Investigación se propone la implementación de un sistema de escritorio para encriptar texto (ya sea desde una interfaz implementada o desde un archivo con extensión txt), con el fin de proteger la información de la empresa Deutsche Pharma. Los usuarios comparten la información por la red, por tal motivo debe estar protegida en caso sea vulnerada. Este sistema, al utilizar un algoritmo criptográfico personalizado da una mayor protección a la información. Por lo tanto, para ejecutar la solución mencionada, se utilizó la metodología ágil SCRUM. Con esta metodología se pudo ejecutar el proyecto de forma eficiente. Asimismo, las herramientas principales para el desarrollo del proyecto propuesto fueron Visual Basic (Programa con el que se desarrollaron las interfaces de los usuarios), el lenguaje de programación C#, Trello (plataforma en la que se pudo desarrollar el Scrumboard), y el método de cifrado de la Regleta que se usó como base para armar el algoritmo criptográfico.

CAPITULO I

ASPECTOS GENERALES

1.1 DEFINICIÓN DEL PROBLEMA

1.1.1 DESCRIPCIÓN DEL PROBLEMA

En la empresa Deutsche Pharma se comparte información confidencial e importante como fórmulas de elaboración de los productos, contratos y otro tipo de datos que se almacenan en un servidor de archivos y es administrada desde la intranet de la empresa. También la información es gestionada a través de la red por correos electrónicos, carpetas virtuales, redes sociales.

Ya que esta información es compartida por medio del internet, es vulnerable, está expuesta a amenazas que afectan la seguridad y privacidad de los datos. Cualquiera podría acceder a ella y manipularla con fines maliciosos, perjudicando a la empresa.

1.1.2 FORMULACIÓN DEL PROBLEMA

¿Es posible analizar, diseñar e implementar un sistema de escritorio que encripte la información?

1.1.3 PROBLEMAS ESPECÍFICOS

1. ¿Es posible analizar y diseñar un sistema de escritorio que permita encriptar los datos utilizando un método de cifrado?
2. ¿Es posible implementar dicho sistema como herramienta de soporte en la empresa

Deutsche Pharma?

1.2 DEFINICIÓN DE LOS OBJETIVOS

1.2.1 OBJETIVO GENERAL

Analizar, diseñar e implementar un sistema de escritorio que permita encriptar la información que se comparte en la red.

El cifrado que se utilizará será construido teniendo como base el método de cifrado de la Regleta. La persona que quiera acceder a dicha información deberá contar con el sistema, y por medio de una clave podrá encriptar y desencriptar la información que requiera.

1.2.2 OBJETIVOS ESPECÍFICOS

1. Analizar y diseñar un sistema que permita encriptar los datos mediante la utilización de herramientas de programación, y el método de cifrado de la Regleta.
2. Implementar el sistema como herramienta de soporte en la empresa Deutsche Pharma.

1.3 JUSTIFICACIÓN DE LA INVESTIGACIÓN

En la actualidad la criptografía es considerada básica en los métodos de seguridad informática. Al tener la información protegida por un cifrado, da la confianza y seguridad de que la información esta salvaguardada.

La información que se maneja en la empresa Deutsche Pharma solo debe ser utilizada por el personal autorizado. Por tal motivo, a pesar de que esté compartida en la red, debe estar protegida por un método de encriptación de datos para que cualquiera que intente acceder a ella no podrá leer la información.

Desde estos puntos de vista, el presente proyecto tiene el fin de proteger la información de la empresa Deutsche Pharma mediante un sistema de encriptación personalizado.

CAPITULO II

FUNDAMENTO TEÓRICO

2.1 ESTADO DEL ARTE

En la actualidad hay muchos sistemas que se encargan de encriptar el contenido de un archivo, como también carpetas. Los programas más comunes son usados en computadoras con el sistema operativo Windows.

A continuación, un listado de las principales aplicaciones de encriptación en el 2016 según el análisis de Victoria Rodríguez.

2.1.1 Steganos Safe

(Rodriguez, 2016) Es uno de los mejores softwares del mercado ya resguarda los archivos y las carpetas en los discos locales, en memorias USB, etc., también en la nube (Como Dropbox y Google Drive). Hace uso del algoritmo AES-XES que tiene 384 bits para encriptar, con esto brinda una encriptación más segura de la lista. Posee una herramienta que genera contraseñas, con la cual la hace invulnerable, permite generar una contraseña en imagen y contiene un teclado virtual con el que protege la información de keyloggers.

2.1.2 AxCrypt

(Rodriguez, 2016) Este programa es fácil de usar y es poderoso. El usuario puede generar un archivo de texto que contiene los datos cifrados para ser enviado por e-mail. Al destinatario también se le deberá enviar la llave que se utilizó. Es un portable.

2.1.3 Gpg4win

(Rodriguez, 2016) Es un programa que utiliza el algoritmo para encriptación OpenPGP. El usuario tiene permitido encriptar la información en la nube, sus correos electrónicos, entre otros datos. El programa es libre y su código es abierto.

2.1.4 DiskCryptor

(Rodriguez, 2016) Este programa solo encripta discos que existen, no cuenta con la opción de crearlos. El DislCryptor contiene algoritmos como el AES, Serpent, etc. Utiliza la encriptación de discos ópticos, también sistemas que son funcionales en pendrivers.

2.1.5. Dekart Private Disk

(Rodriguez, 2016) Este software funciona como volúmenes de HD encriptados. Con solo instalar y activar el programa se puede acceder a sus funciones con facilidad. El programa usa el algoritmo criptográfico AES-256. El cual impide que softwares o usuarios sin autorización accedan a dichos volúmenes.

2.1.6 7-Zip

(Rodriguez, 2016) Este software es conocido como una comprimidora de archivos. Se diferencia en que es de código abierto y es gratuito. Cuenta con la opción de encriptar archivos que este mismo crea, utiliza el algoritmo criptográfico AES-256.

En el momento que se comprimen los archivos, estos pueden ser encriptados. Cuenta también con la opción de bloquear el archivo con una contraseña.

2.1.7 BitLocker Drive Encryption

(Rodriguez, 2016) Este es un sistema que no requiere ser instalado, puede ser colocado en un pendrive y llevado para ser usado en otras computadoras. Utiliza el algoritmo criptográfico AES, puede encriptar archivos, volúmenes y carpetas.

2.1.8 FlashCrypt

(Rodriguez, 2016) Es un software que contiene una llave con 256 bits en su algoritmo criptográfico el cual es el “AES-256”. Este software también tiene la capacidad de comprimir archivos. Es muy útil al momento de hacer uso de servicios en línea para transferir de archivos. También cuenta con la opción de recuperar contraseñas que fueron olvidadas.

2.1.9 Idoo File Encryption

(Rodriguez, 2016) Este software ayuda a prever los accesos que no son permitidos a los archivos que son personales. También puede encriptar los archivos de Microsoft Office, JPG, PDF, mp4, entre otros. Da una protección de la información utilizando una contraseña que se puede recuperar por correo electrónico. Usa el algoritmo criptográfico AES.

2.1.10 TrueCrypt

(Rodriguez, 2016) Es un programa en el que los archivos se pueden encriptar y desencriptar solo si el aplicativo está inicializado. La información encriptada es almacenada en archivos. Se puede acceder al archivo encriptado solo con la contraseña. Utiliza los algoritmos de encriptación AES-256, Twofish y también Serpent.

2.2 MARCO TEÓRICO

2.2.1 Métodos de cifrado

A continuación, una lista de métodos de cifrado mencionado por Heidi Chaves (Chaves Jiménez, 2008) y Luis Rodríguez (Rodríguez Marín):

2.2.1.1 Método de sustitución polialfabética Vigeneré

El cifrado de Vigeneré consta de un cuadro que tiene el alfabeto de 26 letras en filas y columnas, formando un cuadro de 26 x 26. Utiliza una palabra clave que se relaciona con el mensaje (Texto plano) letra con letra (de ser la palabra clave menor al mensaje se repite hasta relacionarse con todas las letras del mensaje). Estos son los pasos por seguir para cifrar:

1. Se busca la letra del mensaje (Texto plano) en la primera fila.
2. Se busca la letra de la clave en primera columna.
3. La letra cifrada se encuentra en la intersección de la columna con la fila.

Estos son los pasos por seguir para descifrar:

1. Se busca la letra de la clave en la primera columna.
2. En la fila de la letra clave se busca la letra cifrada.
3. En la columna de la letra cifrada, se encuentra la letra del mensaje en la primera fila.

Ejemplo:

ENTRADA CLAVE	ENTRADA TEXTO PLANO																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Tabla 1. Tabla de Vigeneré

Mensaje:	V	I	G	E	N	E	R	E
Clave:	V	A	L	O	R	V	A	L
Mensaje cifrado:	Q	I	R	S	E	Z	R	P

Tabla 2. Ejemplo de un texto cifrado en Vigeneré

2.2.1.2 Método por sustitución monoalfabético César

Según Heidi Chaves (Chaves Jiménez, 2008), consiste en reemplazar cada letra de un mensaje a cambio de otra letra perteneciente al criptograma. El cifrado César se basa en utilizar un alfabeto llamado “Mensaje” de 27 letras para buscar la letra del mensaje, y un alfabeto llamado “Criptograma” de 27 letras (empezando por la letra que se encuentra en la posición tres del alfabeto principal) para buscar la letra cifrada.

Estos son los pasos por seguir para cifrar:

1. Se busca la letra del mensaje (Texto plano) en el alfabeto “Mensaje”.

2. La letra cifrada se encuentra en el alfabeto “Criptograma”, en la posición de la letra del mensaje encontrada en el alfabeto “Mensaje”.

Estos son los pasos por seguir para descifrar:

1. Se busca la letra cifrada en el alfabeto “Criptograma”.
2. La letra del mensaje original se encuentra en el alfabeto “Mensaje”, en la posición de la letra cifrada encontrada en el alfabeto “Criptograma”.

Ejemplo:

Mensaje	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**Ñ**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Criptograma	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Tabla 3. Tabla de cifrado César

Mensaje:	C	I	F	R	A	D	O		C	E	S	A	R
Criptograma:	F	L	I	U	D	G	R		F	H	V	D	U

Tabla 4. Ejemplo de un texto cifrado en César

2.2.1.3 Método de la Regleta

El cifrado de la Regleta consta de una plancha rectangular que tiene un alfabeto “Primario” en la parte superior y en la parte inferior (en una cinta o regleta móvil) un alfabeto doble “Secundario” que contiene las letras para armar el cifrado. Para cifrar se ubica la letra inicial del alfabeto “Primario” y se alinea a la letra del texto clave (ubicado en el alfabeto “Secundario”), para luego buscar la letra del mensaje en el alfabeto “Primario” y hallar la letra cifrada ubicada en la parte inferior de dicha letra. Se pueden considerar en el cálculo saltos de acuerdo con un número clave.

Estos son los pasos por seguir para cifrar con una regleta monoalfabética:

1. Se ubica la primera letra del alfabeto “Primario” y se junta con la letra del texto clave.
2. Luego se desplaza el alfabeto “Secundario” la cantidad de espacios indicado por el número clave y en la dirección de este (si es negativo se desliza en dirección izquierda, si es positivo se desliza en dirección derecha), esta parte del cálculo es conocida como saltos.

3. Se busca la letra del mensaje en el alfabeto “Primario”.
4. Se busca la letra cifrada ubicada en el alfabeto “Secundario”, debajo de la letra del mensaje encontrada.

Estos son los pasos por seguir para descifrar:

5. Se ubica la primera letra del alfabeto “Primario” y se junta con la letra del texto clave.
6. Luego se desplaza el alfabeto “Secundario” la cantidad de espacios indicado por el número clave y en la dirección de este (si es negativo se desliza en dirección izquierda, si es positivo se desliza en dirección derecha), esta parte del cálculo es conocida como saltos.
7. Se busca la letra cifrada en el alfabeto “Secundario”.
8. Se busca la letra del mensaje ubicada en el alfabeto “Primario”, encima de la letra cifrada encontrada.

Ejemplo:

	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**Ñ**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U

Tabla 5. Tabla del método de la Regleta

Palabra Clave:	R	E	G	L	E	T	A		
Número Clave:	-2	4	-3						
Mensaje:	**S**	**E**	**G**	**U**	**R**	**I**	**D**	**A**	**D**

Tabla 6. Tabla para cálculo de cifrado con el método de la Regleta

Palabra Clave:	R	E	G	L	E	T	A	R	E
Número Clave:	-2	4	-3	-2	4	-3	-2	4	-3
Mensaje:	**S**	**E**	**G**	**U**	**R**	**I**	**D**	**A**	**D**
Cifrado:	**M**	**E**	**O**	**H**	**R**	**E**	**F**	**Ñ**	**K**

Tabla 7. Tabla de resultados al aplicar el cálculo de cifrado con el método de la regleta

Los alfabetos pueden tener un orden diferente para aumentar la complejidad del cifrado. De acuerdo con el levantamiento de información de la lista anterior, se consideró el método de cifrado de la Regleta como el más adecuado para el desarrollo del proyecto. Esto es por ser más complejo, ya que se puede añadir una clave de texto y una clave numérica de diferentes cifras y direcciones para el cálculo.

2.2.3 Herramientas para el Desarrollo

2.2.3.1 Comparativo de Software de escritorio vs Software WEB

Según “Internet Ya” (Internet ya, 2018) se realizó una comparación entre Software de Escritorio y Software WEB, esto se refleja en la siguiente tabla:

Aplicaciones	Escritorio	WEB
Portabilidad	Se puede usar desde cualquier ubicación solo si es ejecutable.	Se puede usar desde cualquier ubicación.
Internet	Puede funcionar sin internet de acuerdo con su programación.	Depende de una conexión a internet para utilizarlo.
Rendimiento	Tiene una respuesta rápida.	Tiene una respuesta rápida.
Facilidad de instalación	Necesita ser instalado para utilizarlo, o puede ser portable.	No debe ser instalado para utilizarlo.
Seguridad	Se puede configurar para que sea segura. En caso de no usar internet es más seguro.	Se puede configurar para que sea segura.
Sistema operativo	Usualmente se configura para un Sistema Operativo específico.	No es necesario un Sistema Operativo específico.

Tabla 8. Tabla comparativa de Software de escritorio vs. WEB

De acuerdo con el levantamiento de información de la tabla anterior, se consideró el Software de escritorio como el más adecuado para el desarrollo del proyecto. Esto es porque se puede utilizar sin conexión a Internet, también porque puede ser seguro de acuerdo con su programación.

2.2.3.2 Comparativo de Lenguajes de programación

Según Rosado (Rosado, 2019) se realizó una comparación entre los lenguajes de programación Java, C# y Visual Basic. Esto se refleja en la siguiente tabla:

Lenguaje	Fortalezas	Debilidades
Java	• Es un lenguaje orientado a objetos. • Es Multiplataforma. • Por ser orientado a objetos puede desarrollarse en módulos. • Se puede utilizar para la creación de aplicaciones de escritorio.	Ya que es un lenguaje interpretado es un poco lento en comparación con otros lenguajes.
C#	• Es un lenguaje orientado a objetos. • Funciona muy bien en los sistemas operativos Windows. • Su sintaxis es comparable con los lenguajes C y C++.	Se necesita un mínimo de 4 GB de memoria para su instalación.
Visual Basic	• Es un lenguaje orientado a objetos. • Posee un método de programación modular. • Facilita el utilizar la plataforma de los sistemas Windows.	Se necesita una gran cantidad de memoria para su instalación, para que funcione de manera eficiente.

Tabla 9. Tabla de comparativa de Lenguajes de programación

De acuerdo con el levantamiento de información de la tabla anterior, se consideró el lenguaje de programación C# como el más adecuado para el desarrollo del proyecto.

2.2.4 Metodologías SCRUM y RUP

Según Juan Fernández y Sebastián Cadelli (Fernández & Cadelli, 2014) se realizó una comparación de las metodologías SCRUM y RUP en la siguiente tabla:

Aspectos	SCRUM	RUP
Clasificación	Es una metodología ágil.	Es una metodología tradicional.
Ciclo	Los Sprint, es decir las iteraciones, son un ciclo completo.	Tiene cuatro fases, las cuales son: Inicio, Elaboración, Construcción y transición.
Planificación	Los sprints tienen una fecha de entrega indicada por el Scrum Master al realizar la planificación. También contiene el trabajo que se realizará por medio de la estimación de esfuerzo para cada tarea.	Basada en el plan de proyectos formales con muchas iteraciones. Tiene una fecha límite e hitos intermedios.
Alcance	Los objetivos son determinados en el "sprint backlog" durante la planificación, indicando que no pueden ser cambiados.	Se encuentra definido con anterioridad en el documento de alance antes de que inicie el proyecto.
Elementos	• Roles (Product owner, Scrum Master, Team). • Poda de requerimientos. • Product Backlog. • Sprint (Planificación, Sprint backlog, Scrum, estimaciones, builds continuos, revisión del sprint, reunión retrospectiva). • valores (foco, comunicación, respeto).	• Roles (Analistas, Desarrolladores, Gestores, Apoyo, Especialista en pruebas). • Actividades. • Productos/Artefactos (Documento de visión, Diagramas de CU., Diagrama de Clases, Modelo E-R, Diagrama de secuencia, Diagrama de estados, etc.). • Flujos de trabajo (Inicio, Elaboración, Construcción, Transición).
Tipos de Proyectos	Es recomendable para los proyectos que necesitan mejoras rápidas. También	Es excelente para proyectos grandes o de largo plazo. A su vez se puede aplicar a proyectos

	se amoldan a proyectos cuyos requerimientos son flexibles.	con media o alta complejidad. Es ideal cuando se cuenta con requerimientos rígidos que son resistentes a los cambios.
Documentación	Tiene poca documentación.	Es completo y tiene una documentación detallada.
Énfasis	Está enfocada a las personas.	Está enfocada a los procesos.

Tabla 10. Tabla comparativa de SRUM y RUP

De acuerdo con el levantamiento de información de la tabla anterior, se consideró a la metodología SCRUM como la más adecuada para el desarrollo del proyecto. Esto es porque es una metodología ágil y rápida.

2.2.4 Herramienta para Gestión de proyectos

Para este proyecto se utilizará la herramienta de gestión de proyectos Trello. Según el sitio web Gestron (Gestron, 2019) Trello es sencillo de utilizar e intuitivo, es accesible y gratuito (con el uso permitido de las opciones principales) y se accede a ella de forma online. Presenta las siguientes características:

- Se distribuye en columnas o listas independientes
- Las listas se subdividen en entradas denominadas “tarjetas”
- En las tarjetas se pueden crear comentarios, generar checklists, incluir archivos adjuntos, establecer calendarios y alarmas, fechas de vencimiento, etiquetas para diferenciar de un simple vistazo qué tienes que hacer en las tareas
- Permite el trabajo en equipo de forma instantánea y telemática, a tiempo real.

2.3 MARCO CONCEPTUAL

2.3.1 Criptografía

Según Gibrán Granados (Granados, 2006), “es el arte de escribir mensajes en clave secreta”. Proviene de las palabras griegas “kriptos”, es decir oculto y “grafos” escritura.

La criptografía es una ciencia que se encarga de confeccionar dispositivos o funciones capaces de transformar un mensaje claro en cifrado utilizando llaves. Se utiliza el término "cifrar" al convertir la información en cifrado y "descifrar" cuando es lo contrario.

Según Luis Rodríguez (Rodríguez Marín), la ciencia que se encarga de recobrar el mensaje cifrado se llama criptoanálisis y junto a la criptografía conforman la Criptología. La siguiente figura ilustra las partes de la Criptología:

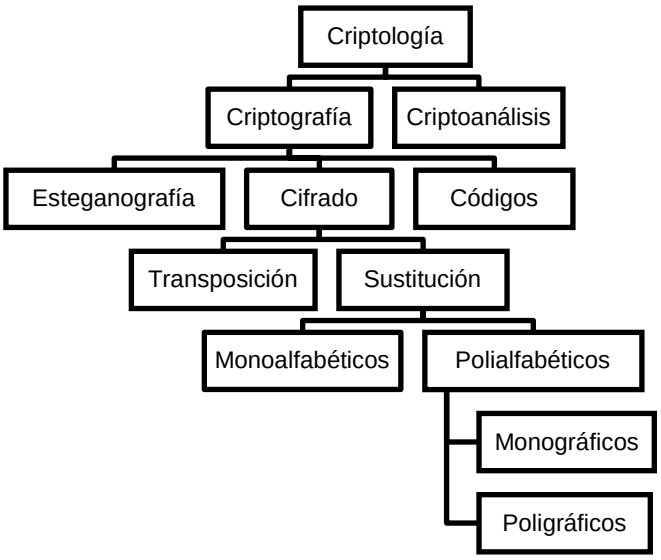


Figura 1. Partes de la Criptología

2.3.2 Cifrado

Según la RAE (Real Academia Española, s.f.) Cifrar es:

"Transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje o texto cuyo contenido se quiere proteger."

Por lo tanto, se entiende por cifrado al texto o mensaje disfrazado o cambiado por otros valores para proteger dicha información.

2.3.3 Seguridad informática

De acuerdo con el diccionario de la RAE (Real Academia Española, s.f.), seguridad es:

"Cualidad de seguro. Dicho de un mecanismo: Que asegura algún buen funcionamiento, precaviendo que este falle, se frustre o se violente."

Por lo tanto, se entiende por Seguridad Informática al conjunto de reglas, planes y acciones que garantizan la confidencialidad, integridad y disponibilidad, resguardan la información.

Según Gibrán Granados (Granados, 2006) los principios básicos de la seguridad informática son:

- La confidencialidad, consiste en que solo los usuarios con autorización puedan acceder a la información.
- La integridad, consiste en que solo el usuario autorizado pueda crear o modificar la información y quede un registro lo realizado.
- La disponibilidad, consiste en que el usuario pueda acceder a dicha información cuando lo requiera.

2.3.4 SCRUM

Según Fernández y Candelli en su tesina (Fernández & Cadelli, 2014) indican que SCRUM es una metodología ágil para la gestión de proyectos. Tiene como objetivo prioritario el elevar al máximo la productividad de un equipo. Esta metodología se enfoca en los valores y las prácticas de gestión. Asigna la responsabilidad de tomar decisiones al equipo de trabajo concerniente a la forma más productiva de trabajar.

Fue desarrollada por Jeff Sutherland y, posteriormente, formalmente elaborada por Ken Schwaber.

Esta metodología se basa en los siguientes principios:

- Dar mayor privilegio al valor de la gente que al valor de los procesos.
- Presentar un software funcional lo en un tiempo óptimo.
- Presentar predisposición y respuesta al cambio.
- EL tener como base la comunicación y colaboración en el equipo.
- Mantener una comunicación verbal y directa entre los involucrados del proyecto.
- Eliminar artefactos que no son necesarios en la gestión del proyecto.

2.3.5 RUP

Según Fernández y Candelli en su tesina (Fernández & Cadelli, 2014) indican que RUP "Proceso Unificado Racional (Rational Unified Process en inglés)" es un proceso de desarrollo de software que junto con el Lenguaje Unificado de Modelado (UML), constituyen una metodología estándar común mente utilizada para el análisis, implementación y documentación de sistemas orientados a objetos. RUP trata de un conjunto de metodologías que se adaptan al contexto y a las necesidades de cada organización, que define claramente quien, cómo, cuándo y qué debe hacerse en el proyecto.

RUP es un proceso para el desarrollo de un proyecto de software que define claramente quien, cómo, cuándo y qué debe hacerse en el proyecto.

Fases de desarrollo de RUP:

RUP comprende las siguientes fases para el desarrollo de software:

1) Inicio

2) Elaboración

3) Construcción

4) Transición

2.3.6 Gestor de proyectos

Según el sitio web de Gestron (Gestron, 2019) es una herramienta que permite aclarar las rutinas de trabajo de los proyectos. Ayuda a tener el proyecto organizado para cumplir con el cronograma de actividades. Entre ellos están Trello y Kanban, las cuales son fáciles de usar para todo tipo de proyectos.

2.4 MARCO METODOLÓGICO

La metodología que se empleará en este Trabajo de Investigación es Scrum, conocida como ágil. Es un marco de trabajo que proporciona una serie de herramientas y roles para, de una forma iterativa, poder ver el progreso y los resultados de un proyecto. Por tal motivo, en este punto, se presentará con más detalle.

2.4.1 Metodología SCRUM

Según la Guía de SCRUM (Satpathy, 2017) se tienen los siguientes puntos:

SCRUM es una metodología flexible y ágil para realizar la gestión y el desarrollo de software. En este proceso se aplican de manera constante un conjunto de buenas prácticas para realizar un trabajo colaborativo, en equipo y de esta manera poder conseguir el mejor resultado posible de un proyecto.

Con esta metodología el cliente ve crecer su proyecto gracias a las iteraciones recurrentes, le permite también de reformar los objetivos del negocio en cualquier momento.

En SCRUM se elaboran tanto entregas parciales como regulares del producto final.

2.4.2 Beneficios

- **Entrega mensual o quincenal de resultados**
- **Flexibilidad a cambios**

  La metodología está diseñada para acoplarse a los diferentes cambios que puedan surgir de los requerimientos que serán del interés de las necesidades del cliente.

- **Reducción del Time to Market**

  El cliente puede hacer uso de las funcionalidades más relevantes del proyecto antes de que este esté finalizado.

- **Mayor calidad del software**

  Gracias a las iteraciones donde se obtiene versiones funcionales se obtiene un producto de mayor calidad.

- **Mayor productividad**

El equipo de trabajo es autónomo, ellos mismos eligen la forma de organizarse. Son autónomos.

- **Reducción de riesgos**

2.4.3 Roles de Scrum

- **Product Owner**

  Es la persona donde cae la responsabilidad del éxito del producto. Sus responsabilidades son:

  - Definir la visión del producto, dónde se está dirigiendo el equipo de desarrollo.

  - Gestionar las expectativas de los stakeholders.

  - Juntar los requerimientos.

  - Definir y tener conocimiento sobre las características funcionales del producto.

  - Generar y mantener el plan de entregas (reléase plan)

  - Diagnosticas las importancias de cada una de las características (prioridades).

  - Cambiar las prioridades de las características según el proyecto va avanzando.

  - Poder Aceptar y también descartar el producto desarrollado durante el Sprint y proveer feedback para su crecimiento.

  - Ser partícipe de la revisión del Sprint en compañía de los miembros que conforma el equipo.

- **Equipo de Desarrollo**

  El equipo de desarrollo se encuentra formado por el personal imprescindible para la construcción o desarrollo del producto.

  El equipo de desarrollo se encarga de su propia organización, no existe un líder. El equipo es quien designa como se realizará el trabajo y como resolverá si en caso se presentes problemas.

- **SCRUM Master**

  Es el líder del equipo en la gestión de proyectos. Hace cumplir a tos los

participantes del proyecto con los procesos de Scrum.

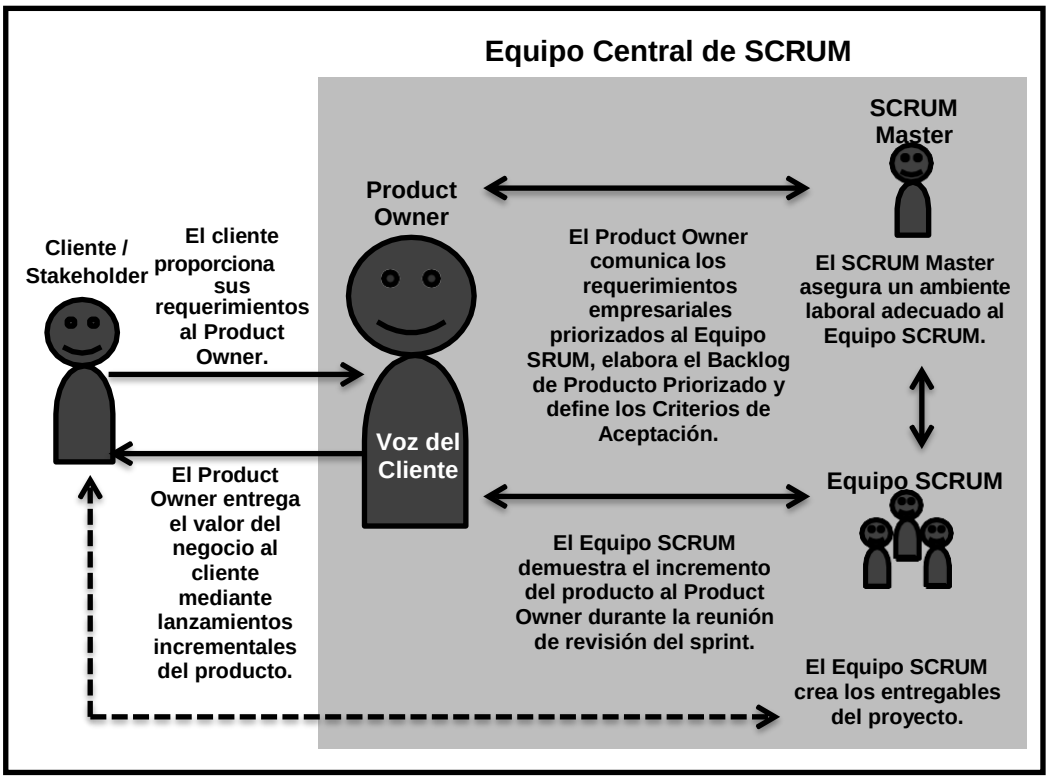


Figura 2. Organización en SCRUM

2.4.4 Elementos de Scrum

El proceso de Scrum contiene algunos elementos formales que de tal manera se pueda avanzar un proyecto de desarrollo:

Product Backlog

Es uno de los elementos más importante de Scrum, el backlog es una lista de ítems o características del producto a construir, sostenible y cuyas prioridades es hecha por el Product Owner.

Es importante definir la priorización de cada característica ya que será el orden en que el equipo de trabajo transformará en un producto funcional terminado.

Sprint Backlog

Es un conjunto de tareas las cuales las realiza el equipo en la reunión de planificación de la iteración.

El Sprint Backlog es un paquete de PBIs (ítems del producto) que fueron elegidos con la

finalidad de trabajarlos durante un Sprint, en unión con las tareas que el equipo de desarrollo ha determinado que debe realizar para poder elaborar un incremento funcional entregable al finalizar el Sprint.

Increment

Es un avance funcional potencialmente entregable, debe ser el resultado de cada Sprint.

Incremento funcional

Se dice que es un incremento o avance funcional debido a que es una característica funcional modificada o recientemente elaborada de un producto que está construyéndose de una forma evolutiva.

Potencialmente entregable

Se dice que es potencialmente entregable porque se realiza una validación y verificación de cada una de las características del producto, en donde se determina que puede ser entregada al usuario si así lo estipula.

2.4.5 Eventos de Scrum

Sprint

Sprint son las iteraciones que se realizan. Scrum es un proceso de desarrollo incremental e iterativo eso quiere decir que el producto se elabora teniendo avances funcionales presentados en lapsos cortos de tiempo para obtener a menudo y hacer uso de los feedbacks.

Los Sprints duran aproximadamente entre 1 a 4 semanas, siendo 2 o 3 semanas lo más habitual. Se recomienda establecer la duración de los Sprint al comenzar el proyecto y mantenerlo constante durante el desarrollo del producto.

Sprint Planning (Planificación de Sprint)

Al iniciar cada Sprint se habitúa realizar una reunión de planificación del Sprint donde el equipo de desarrollo y Product Owner generarán acuerdos y compromisos respecto al alcance del Sprint.

Dicha reunión de planificación está compuesta en dos partes, la primera parte estratégica

y orientada en el “qué” y la segunda parte táctica enfocada en el “cómo”.

- Primera parte de la reunión (reunión de 4 horas como máximo)

  - El cliente hace presente al equipo los requisitos del proyecto a realizarse, establece nombre a la meta de la iteración y propone requisitos de mayor prioridad a desarrollarse.

  - El equipo analiza la lista, esclarece al cliente las dudas y selecciona los objetivos más importantes que se compromete a completar en la iteración.

- Segunda parte de la reunión (reunión de 4 horas como máximo)

  El equipo planifica la iteración, elabora la táctica que le permitirá conseguir el mejor resultado, la forma en la que llevará adelante el trabajo.

Scrum Diario

A la reunión diaria asiste el equipo de trabajo y el ScrumMaster. Se realiza las siguientes peguntas que se responderán por turnos:

1. ¿Desde la última reunión que he realizado o avanzado hasta el día de hoy?
2. ¿Desde ahora hasta que haya la próxima reunión diaria, ¿cuáles serán las tareas en las que trabajaré?
3. ¿Qué obstáculos o dificultades tengo?

Cabe resaltar que esta reunión es enriquecedora ya que la comunicación y el diálogo entre los integrantes del equipo de desarrollo se intensifican.

Al realizar la primera pregunta, se verifica si los integrantes del equipo de desarrollo han cumplido con sus compromisos respectivos.

En la segunda pregunta, se da a conocer los nuevos compromisos.

Finalmente, la tercera pregunta da a conocer los obstáculos que se les ha presentado a los integrantes del equipo de desarrollo que serán resueltos posteriormente y será responsabilidad del Scrum Master de que sean resueltas lo más antes posible.

2.4.6 Roles de usuario

Para analizar el sistema, se debe identificar los usuarios posibles con el que el sistema

poseerá.

2.4.7 Historias de Usuario

En los proyectos de desarrollo de software, la comunicación entre el cliente y el desarrollador solía hacerse mediante documentación más conocida como especificaciones funcionales que causaban malentendidos y muchas veces el software elaborado no era con lo que se esperaba.

Una razón por la cual las especificaciones funcionales transmitidas como una forma de comunicación no conllevan a resultados esperados o agradables es debido a que no existe una comunicación en persona. Las historias de usuario son especificaciones funcionales que incitan a un dialogo para que el detalle no sea un remplazo sino más bien una consecuencia.

Una historia de Usuario lo integran 3 elementos, llamados como “las tres Cs”.

- **Card**

  Toda historia de usuario debe ser escrita en una ficha pequeña, si no alcanzara, se debería compartir la información presencialmente.

- **Conversación**

  Toda historia debe ser conversada con el Product Owner. Una comunicación presencial que permita intercambiar tanto opiniones, pensamientos y sentimientos (muy a parte de la información).

- **Confirmación**

  Toda historia de usuario debe estar muy bien explicada de tal manera que el equipo de desarrollo comprenda qué es lo ha de desarrollar.

Los beneficios que trae este modo de redacción son:

- Ponerse en el lugar del usuario, la persona quien lee una determinada historia de usuario comprende mejor la necesidad del usuario.

- Ayuda a priorizar las funcionalidades.

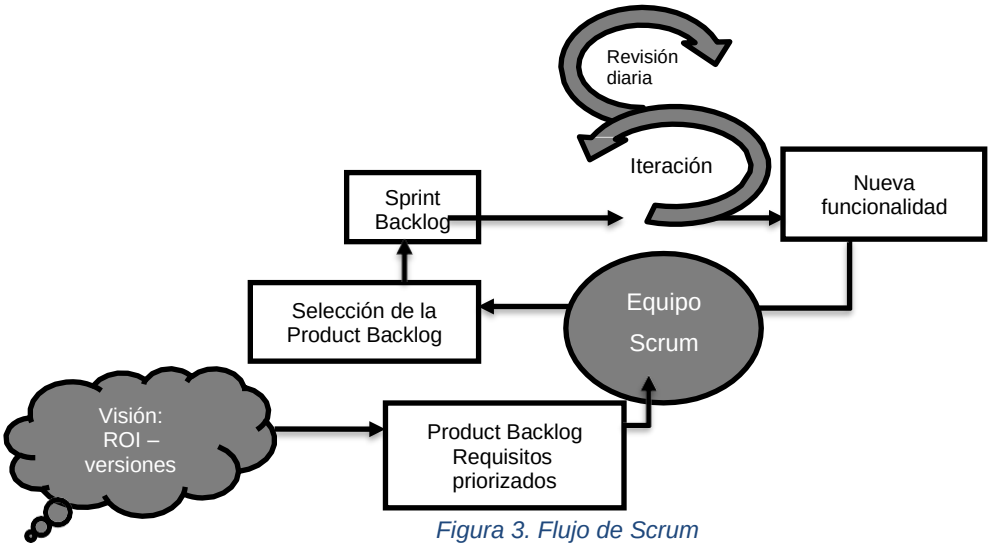


Figura 3. Flujo de Scrum

Capítulo	Fase	Procesos fundamentales de Scrum
8	Inicio	1. Crear la visión del proyecto 2. Identificar al Scrum Master y Stakeholder(s) 3. Formar Equipos Scrum 4. Desarrollar épica(s) 5. Crear el Backlog Priorizado del Producto 6. Realizar la planificación de lanzamiento
9	Planificación y estimación	7. Crear historias de usuario 8. Estimar historias de usuario 9. Comprometer historias de usuario 10. Identificar tareas 11. Estimar tareas 12. Crear el Sprint Backlog
10	Implementación	13. Crear entregables 14. Realizar Daily Standup 15. Refinar el Backlog Priorizado del Producto
11	Revisión y retrospectiva	16. Demostrar y validar el sprint 17. Retrospectiva del sprint
12	Lanzamiento	18. Enviar entregables 19. Retrospectiva del proyecto

Figura 4. Procesos funcionales de SCRUM

2.5 MARCO LEGAL

A continuación, se detalla el marco legal que será considerado para desarrollar este proyecto.

2.5.1 Normativa aplicable a las licencias de uso de software

Para desarrollar el software descrito en este documento, se debe utilizar un software propietario, esto es respaldado por el siguiente Marco Legal:

2.5.1.1 Marco Legal Internacional

- Tenemos el tratado de OMPI que trata de los Derechos de Autoría. http://www.wipo.int/treaties/es/ip/wct/trtdocs_wo033.html
- También la decisión Andina 351, correspondiente a la Comunidad Andina de Naciones. (17 de diciembre de 1993) Es un régimen Común que trata sobre los Derechos de Autoría y los Derechos Conexos. http://www.wipo.int/wipolex/es/text.jsp?file_id=223497

2.5.1.2 Marco Legal Nacional

- Contamos con el decreto Legislativo 822: Trata de la ley sobre los Derechos de Autoría. http://www.wipo.int/wipolex/es/text.jsp?file_id=129302
- También se contempla la ley Nro. 28571: Menciona la modificación de los artículos 188° y 189° correspondientes al Decreto Legislativo Nro. 822, Trata de la ley sobre los Derechos de Autoría. http://www.wipo.int/wipolex/es/text.jsp?file_id=183056
- Se cuenta con el reglamento del Registro Nacional de los Derechos de Autoría y los Derechos Conexos; y con la Resolución Jefatural Nro. 0276-2003/ODA-INDECOPI. http://www.wipo.int/wipolex/es/details.jsp?id=6492
- As su vez tenemos a la ley Nro. 29316: Modifica, incorpora y regula disposiciones con el fin de poder implementar el Acuerdo de Promoción Comercial entre Perú y Estados Unidos. http://www.wipo.int/wipolex/es/text.jsp?file_id=179604

Debido a estas leyes, es obligatorio para la empresa el comprar las licencias de software que se requieran para la implementación de un proyecto. El uso de softwares propietarios sin poseer las licencias correspondientes tiene las siguientes sanciones:

- El pago de multas corresponde a 180 UIT (unidades impositivas tributarias).
- Las sanciones penales corresponden a 8 años de prisión, según se establece en el Código Penal.

Fuente: INDECOPI

- https://www.indecopi.gob.pe/-/indecopi-lanza-v-campana-de-software-legal-para-incentivar-el-usode-programas-informaticos-legales
- http://www.compralegalyoriginal.pe/pirateria.html

2.5.2 Normativa aplicable a la protección de la información

El Observatorio Iberoamericano de Protección de Datos menciona, en un artículo publicado el año 2013, otras Leyes y Normas que se aplican al resguardo de la información:

- Tenemos a la ley de los delitos informáticos (LEY Nro. 30096): http://www.leyes.congreso.gob.pe/Documentos/Leyes/30096.pdf
- También la ley de manifestación de la voluntad por medio electrónico (LEY Nro. 27291): https://docs.peru.justia.com/federales/leyes/27291-jun-23-2000.pdf
- A su vez la ley antispam (LEY Nro. 28493): Esta ley regula el uso de los correos electrónicos comerciales no solicitados (SPAM). http://www2.congreso.gob.pe/sicr/cendocbib/con2_uibd.nsf/DCD93A0451E78406052577E600635179/$FILE/Ley_28493_correo_electronico_spam.pdf

2.5.3 Estándares de la Organización Internacional de Estándares (ISO)

Se cuenta con los siguientes estándares:

- ISO/IEC 9979 Tecnología de información - Técnicas seguras - Procedimiento para el registro de algoritmos criptográficos.
- SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI), Norma Técnica Colombiana
- NTC-BS-7799-2 (ICONTEC) CÓDIGO DE LAS BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, Norma Técnica Colombia NTC-ISO/IEC 17799 (ICONTEC)

CAPITULO III

DESARROLLO DE LA APLICACIÓN

3.1 MODELAMIENTO

3.1.1 INICIO

3.1.1.1 CREAR LA VISIÓN DEL PROYECTO

El presente proyecto tiene como visión el proteger la información de la empresa Deutsche Pharma realizando el análisis, diseño e implementación de un sistema de escritorio que permita encriptar la información que se comparte en la red.

3.1.1.2 CREAR EL BACKLOG PRIORIZADO DEL PRODUCTO

La persona responsable de este proceso es el Product Owner, representa a los usuarios y clientes del producto, también ayudará en el direccionamiento del producto.

Requerimientos de los usuarios identificados:

Código	Requerimiento	Prioridad
R01	El sistema debe permitir ingresar texto a encriptar.	Alta
R02	Debe permitir encriptar texto contenido en un archivo.	Media

Tabla 11. Backlog priorizado del producto

3.1.1.3 REALIZAR LA PLANIFICACIÓN DEL LANZAMIENTO

El SCRUM Master es quien lidera las reuniones para planificar el lanzamiento del producto, así como del cumplimiento de este.

Para el desarrollo del cronograma de Actividades se consideró solo trabajar en el proyecto de lunes a viernes y 4 horas diarias. Por lo tanto, el proyecto cuenta con un solo Sprint, el Sprint 01, el cual tiene una duración de 12 días con fecha de inicio 01/07/2019 y con fecha de fin 16/07/2019.

Historia de Usuario	Tarea	Fecha inicio	Días	Fecha fin
HU01	T01	01/07/2019	1	01/07/2019
HU01	T02	02/07/2019	3	04/07/2019
HU01	T03	05/07/2019	1	05/07/2019
HU01	T04	08/07/2019	2	09/07/2019
HU02	T05	10/07/2019	2	11/07/2019
HU02	T06	12/07/2019	3	16/07/2019

Tabla 12. Cronograma de Actividades del Sprint 01

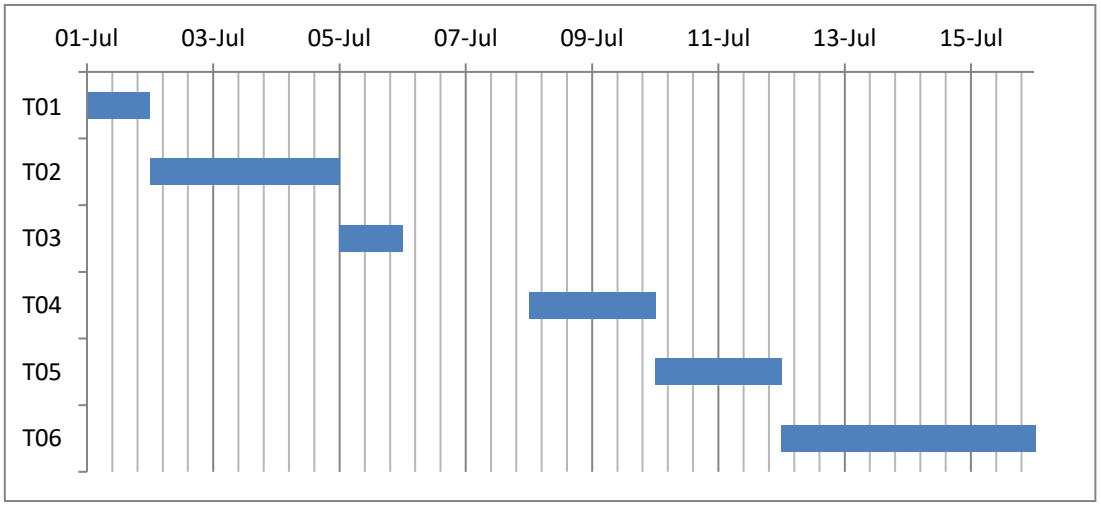


Figura 5. Diagrama de Gantt del Sprint 01

3.1.2 PLANIFICACIÓN Y ESTIMACIÓN

3.1.2.1 CREAR HISTORIAS DE USUARIO

De acuerdo con el Backlog priorizado del producto se tienen las siguientes Historias de usuario:

Historia de Usuario	
ID	HU01
Nombre	Encriptar texto ingresado
Prioridad	Alta
Riesgo	Bajo
Descripción	Como usuario quiero encriptar y desencriptar un texto ingreso en el sistema.
Validación	- Quiero que se utilice un cifrado seguro. - Quiero encriptar cualquier tipo de palabra u oración con caracteres especiales. - Quiero una clave al encriptar por seguridad.

Tabla 13. Historia de usuario HU01

Historia de Usuario	
ID	HU02
Nombre	Encriptar texto que se encuentra en un archivo de texto específico.
Prioridad	Media
Riesgo	Bajo
Descripción	Como usuario quiero encriptar y desencriptar un texto que se encuentra en un archivo especifico en el sistema.
Validación	- Quiero que se utilice un cifrado seguro. - Quiero encriptar cualquier tipo de palabra u oración con caracteres especiales que se encuentren en el archivo seleccionado. - Quiero una clave al encriptar por seguridad.

Tabla 14. Historia de usuario HU02

3.1.2.2 ANALISIS

Se realizó un análisis de las Historias de Usuario para poder realizar la estimación de cada una. Se utilizaron diagramas de flujo de los procesos a realizar para cumplir cada Historia de Usuario y también se elaboraron prototipos.

3.1.2.2.1 DIAGRAMA DE FLUJO

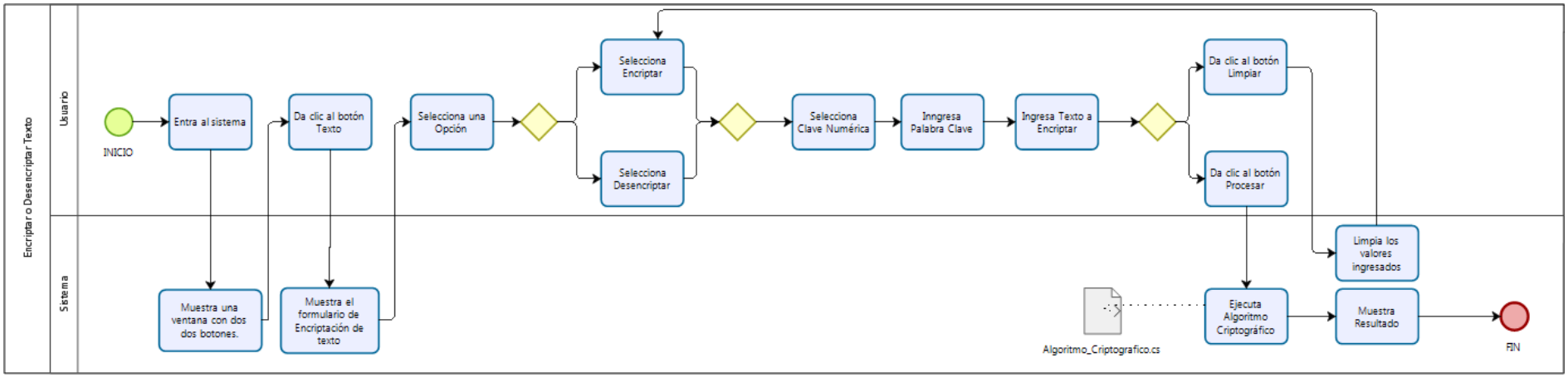


Figura 6. Encriptar o Desencriptar Texto

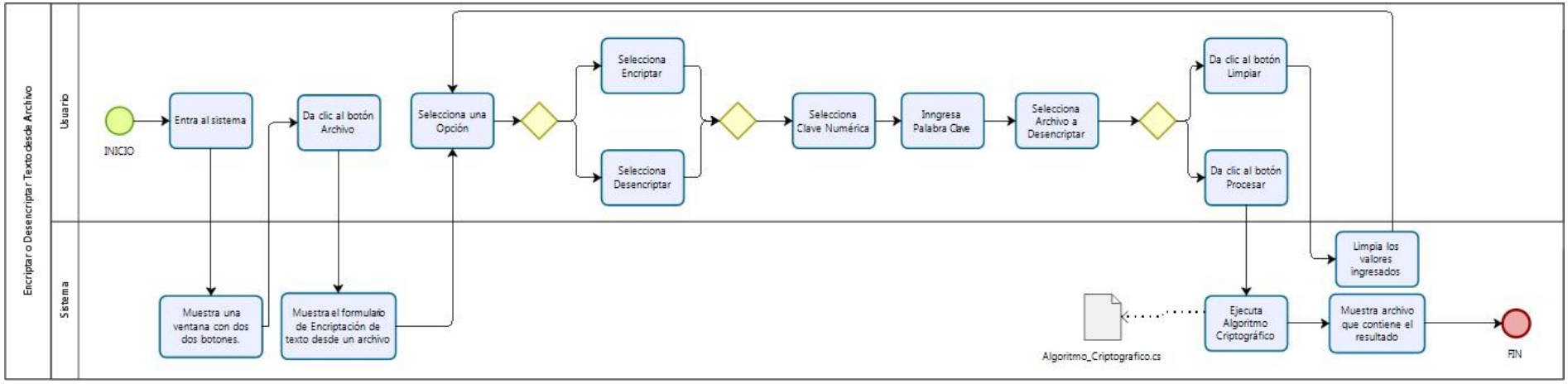


Figura 7. Encriptar o Desencriptar Texto desde Archivo

3.1.2.2.2 PROTOTIPOS

- Interfaz gráfica de inicio del programa

Figura 8. Interfaz gráfica de inicio del programa

- Interfaz gráfica para encriptar y desencriptar un texto ingresado.

Figura 9. Interfaz gráfica para encriptar y desencriptar un texto ingresado.

- Interfaz gráfica para encriptar y desencriptar un texto contenido en un archivo de texto seleccionado.

Figura 10. Interfaz gráfica para encriptar y desencriptar un texto contenido en un archivo de texto seleccionado.

3.1.2.3 ESTIMAR HISTORIAS DE USUARIO

Los que participaron de la estimación de las Historias de Usuarios son:

Miembro A = SCRUM Master.

Miembro B = Equipo SCRUM (Analista Programador).

Miembro C = Equipo SCRUM (QA Tester).

Historia de Usuario	Miembro			Estimación Media	Prioridad
	A	B	C		
HU01	20	25	22	22.33333333	Alta
HU02	15	18	16	16.33333333	Media

Tabla 15. Estimación de Historias de usuarios

El tiempo estimado para la elaboración del proyecto es de 38.66 horas. Si se consideran 4 horas de trabajo por día, se interpretan entre 10 y 12 días aproximadamente.

3.1.2.4 COMPROMETER HISTORIAS DE USUARIO

El SCRUM Master asigna un responsable para cada Historia de usuario de acuerdo con la complejidad del desarrollo del proyecto y a las capacidades de los miembros de su equipo.

Historia de Usuario	Estimación Media	Prioridad	Responsable
HU01	22,33333333	Alta	Analista Programador
HU02	16,33333333	Media	Analista Programador

Tabla 16. Estimación de Historias de Usuarios

3.1.2.5 IDENTIFICAR TAREAS

El Equipo SCRUM es el encargado de identificar las tareas de cada Historia de Usuario.

Tarea	T01
Historia de Usuario	HU01
Estado	No iniciada
Descripción	Diseñar y desarrollar la interfaz gráfica de inicio del programa.

Tabla 17. Tarea T01 de la Historia de Usuario HU01

Tarea	T02
Historia de Usuario	HU01
Estado	No iniciada
Descripción	Crear el algoritmo Algoritmo_Criptografico.cs de encriptación y desencriptación de datos.

Tabla 18. Tarea T02 de la Historia de Usuario HU01

Tarea	T03
Historia de Usuario	HU01
Estado	No iniciada
Descripción	Diseñar y desarrollar la interfaz para encriptar y desencriptar un texto ingresado.

Tabla 19. Tarea T03 de la Historia de Usuario HU01

Tarea	T04
Historia de Usuario	HU01
Estado	No iniciada

Descripción	Utilizar el algoritmo Algoritmo_Criptografico.cs de encriptación y desencriptación de datos para texto ingresado.

Tabla 20. Tarea T04 de la Historia de Usuario HU01

Tarea	T05
Historia de Usuario	HU02
Estado	No iniciada
Descripción	Diseñar y desarrollar la interfaz para encriptar y desencriptar un texto contenido en un archivo de texto seleccionado.

Tabla 21. Tarea T05 de la Historia de Usuario HU02

Tarea	T06
Historia de Usuario	HU02
Estado	No iniciada
Descripción	Utilizar el algoritmo Algoritmo_Criptografico.cs de encriptación y desencriptación de datos para texto en archivo.

Tabla 22. Tarea T06 de la Historia de Usuario HU02

3.1.2.6 ESTIMAR TAREAS

Los que participaron de la estimación de las Tareas son:

Miembro A = SCRUM Master.

Miembro B = Equipo SCRUM (Analista Programador).

Miembro C = Equipo SCRUM (QA Tester).

Historia de Usuario	Tarea	Miembro			Estimación Media	Prioridad
		A	B	C		
HU01	T01	1	2	2	1,666666667	Alta
HU01	T02	9	12	9	10	Alta
HU01	T03	4	4	5	4,333333333	Alta
HU01	T04	6	7	6	6,333333333	Alta
HU02	T05	8	8	6	7,333333333	Media
HU02	T06	7	10	10	9	Media

Tabla 23. Estimación de las Tareas

Nota: La estimación es en horas.

3.1.2.7 CREAR EL SPRINT BACKLOG

El proyecto solo cuenta con el Sprint 01, el cual está conformado por las siguientes tareas:

Spring	Historia de Usuario	Tarea	Fecha inicio	Días	Fecha fin
Spring 01	HU01	T01	01/07/2019	1	01/07/2019
	HU01	T02	02/07/2019	3	04/07/2019
	HU01	T03	05/07/2019	1	05/07/2019
	HU01	T04	08/07/2019	2	09/07/2019
	HU02	T05	10/07/2019	2	11/07/2019
	HU02	T06	12/07/2019	3	16/07/2019

Tabla 24. Spring Backlog del proyecto

Se utilizará el programa Trello para crear el Scrumboard del Sprint 01. Se crearon las secciones “Por hacer”, “En proceso”, “En prueba” y “Terminado”.

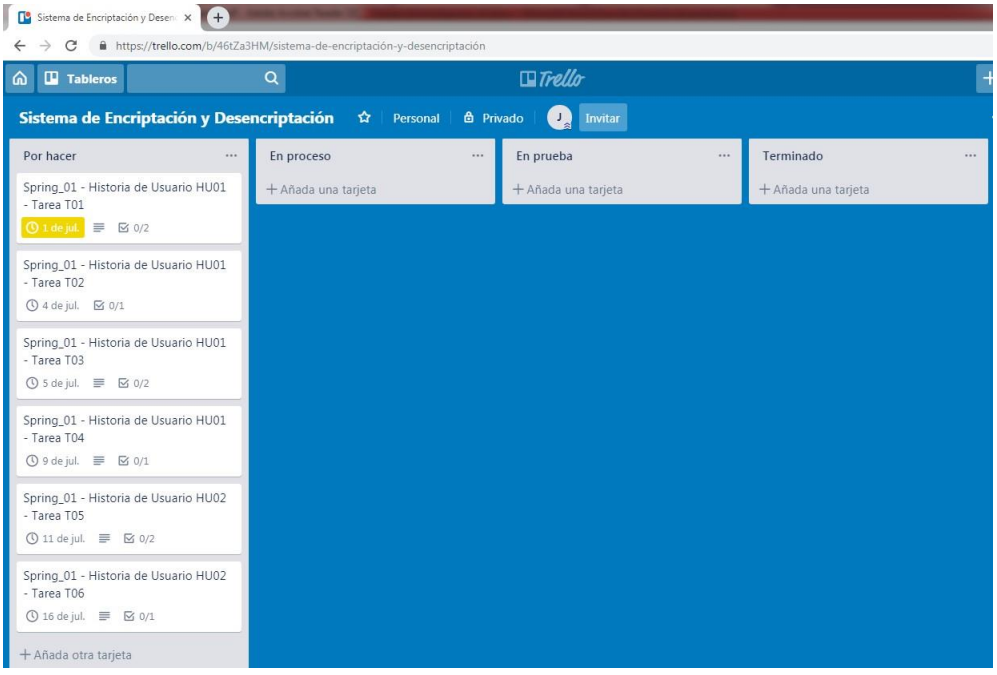


Figura 11. Scrumboard del Sprint 01 en Trello

3.2 DESARROLLO

3.2.1 IMPLEMENTACIÓN

3.2.1.1 CREAR ENTREGABLES

El responsable del desarrollo de las Historias de Usuario es el Analista Programador, el cual debe realizar las tareas en el tiempo estimado.

A continuación, se presenta el cumplimiento de cada tarea con los respectivos entregables.

Desarrollo de la tarea T01:

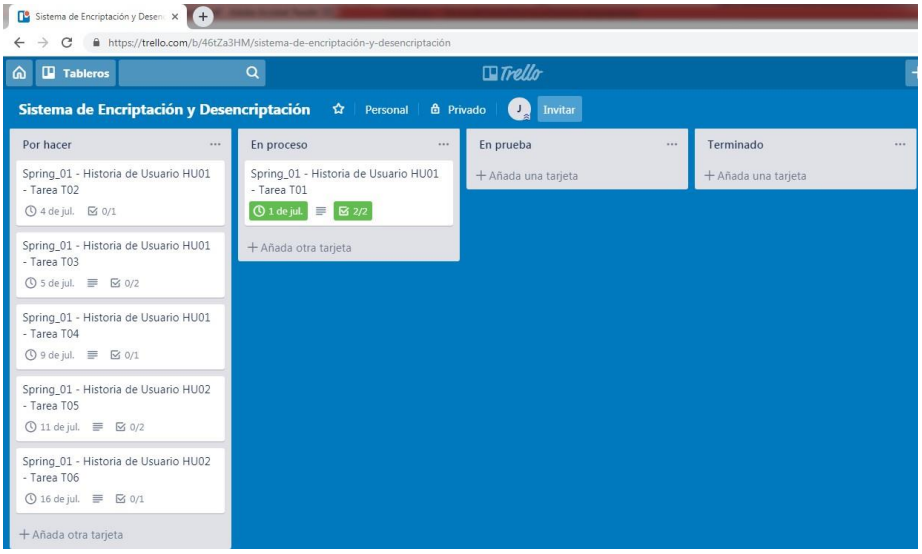


Figura 12. Scrumboard de la tarea T01 en proceso.

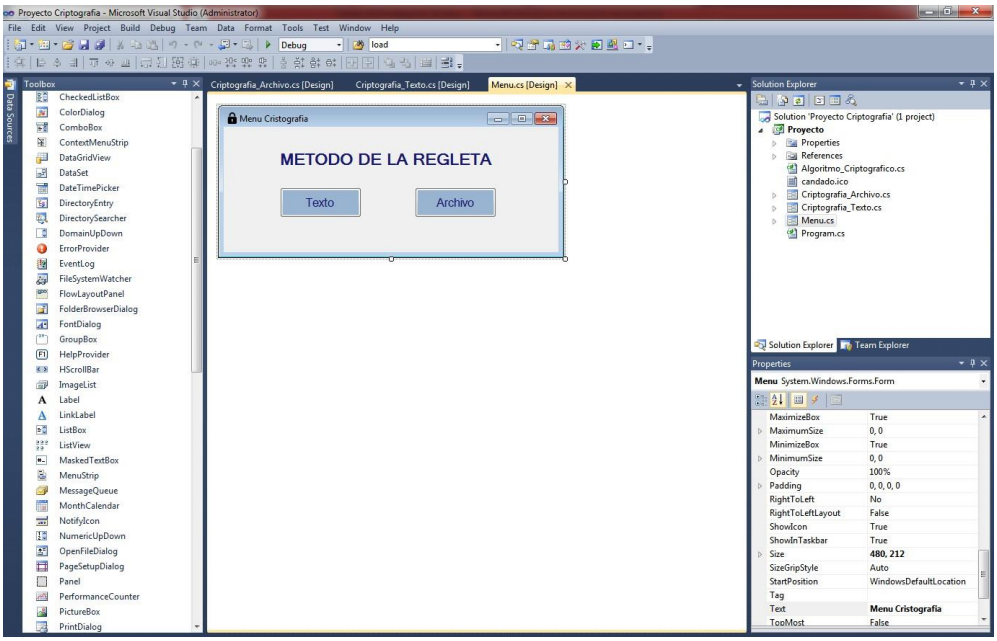


Figura 13. Entregable de la tarea T01

Desarrollo de la tarea T02:

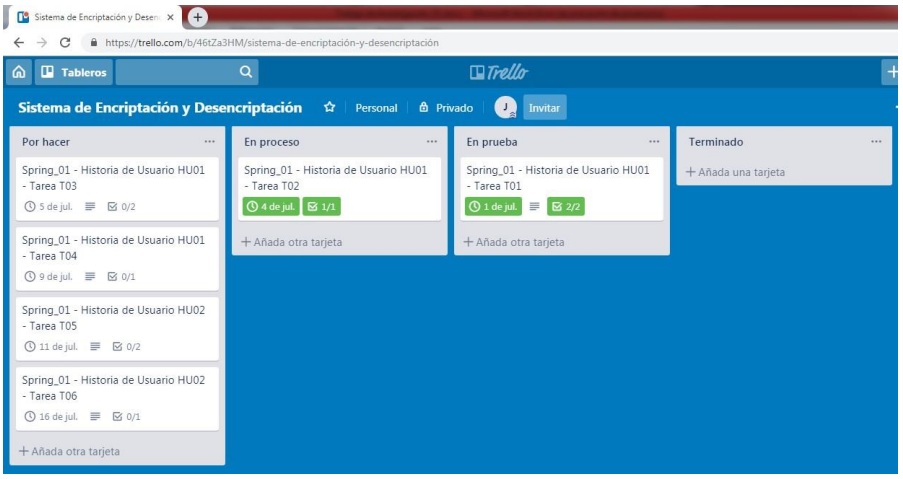


Figura 14. Scrumboard de la tarea T02 en proceso.

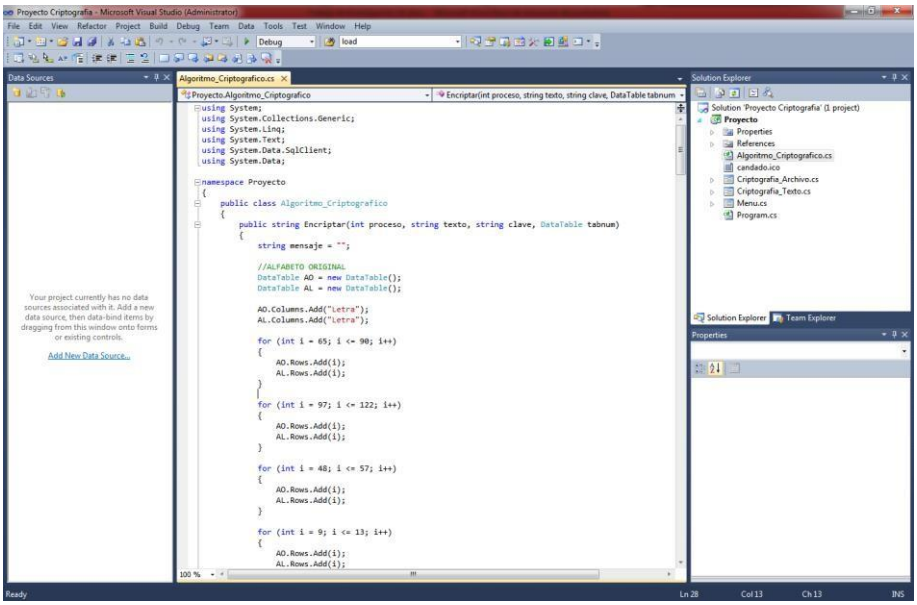


Figura 15. Entregable de la tarea T02

Desarrollo de la tarea T03:

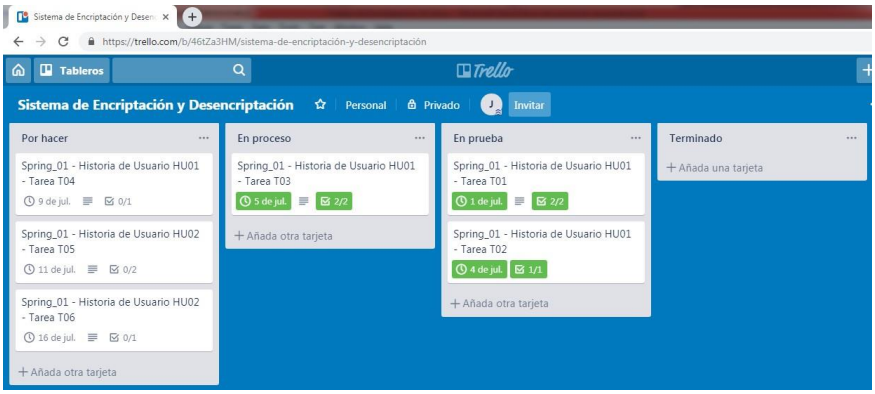


Figura 16. Scrumboard de la tarea T03 en proceso.

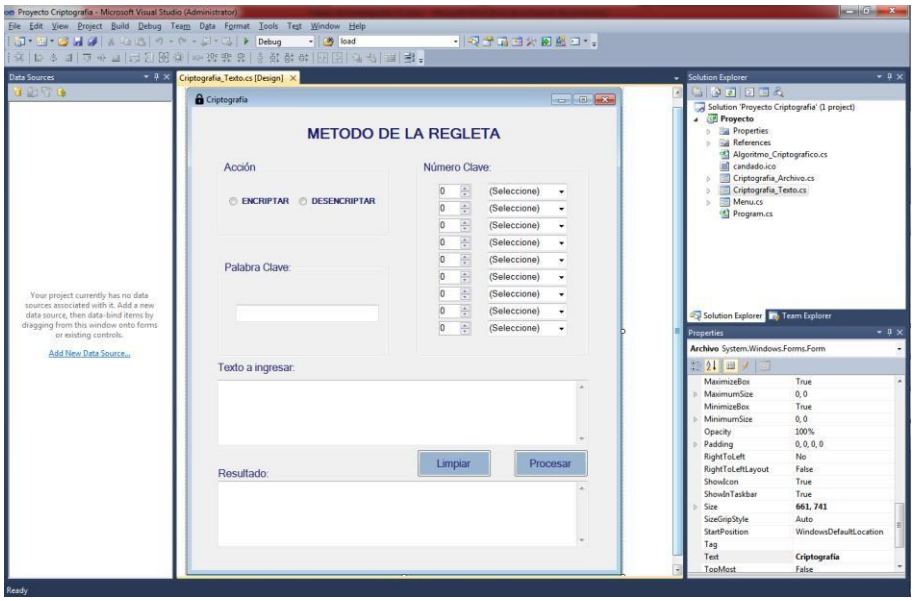


Figura 17. Entregable de la tarea T03

Desarrollo de la tarea T04:

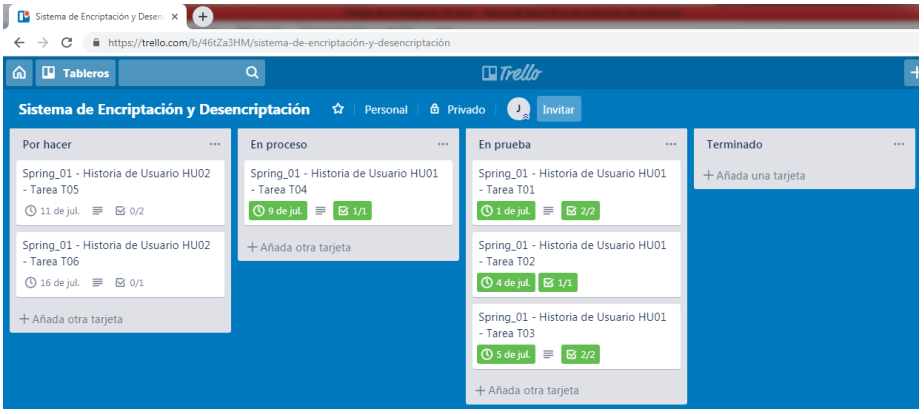


Figura 18. Scrumboard de la tarea T04 en proceso.

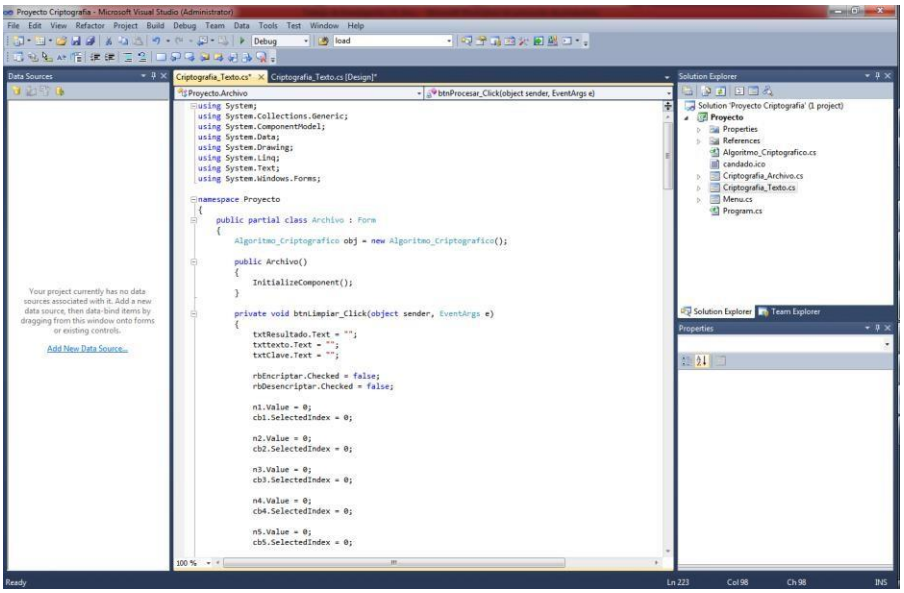


Figura 19. Entregable de la tarea T04

Desarrollo de la tarea T05:

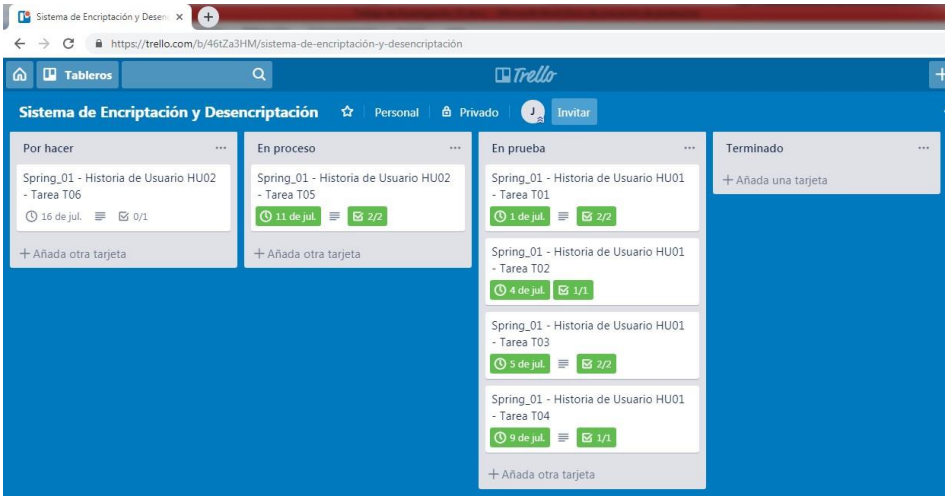


Figura 20. Scrumboard de la tarea T05 en proceso.

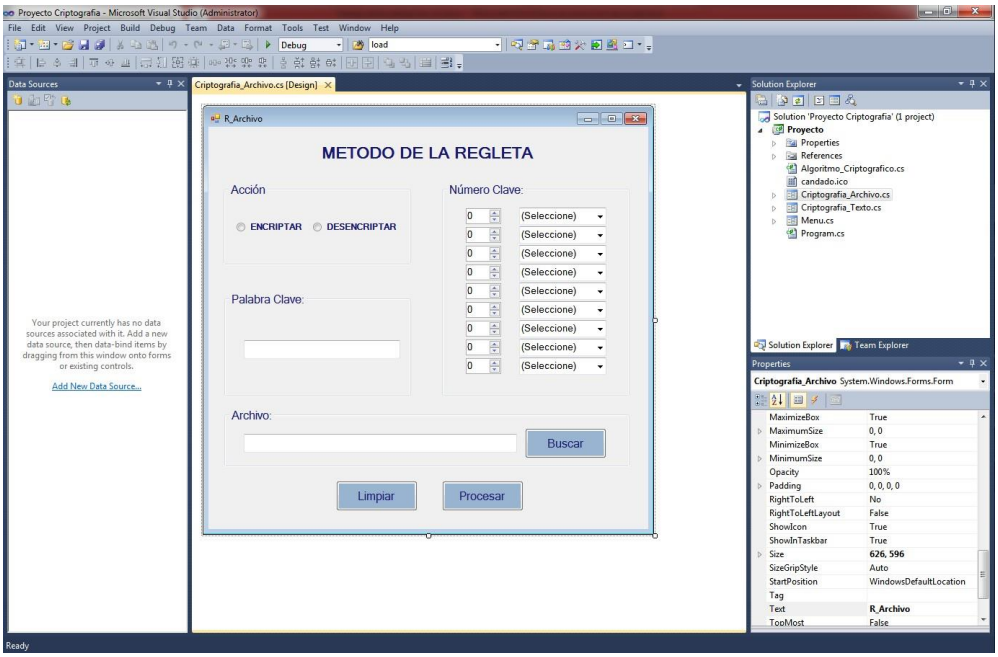


Figura 21. Entregable de la tarea T05

Desarrollo de la tarea T06:

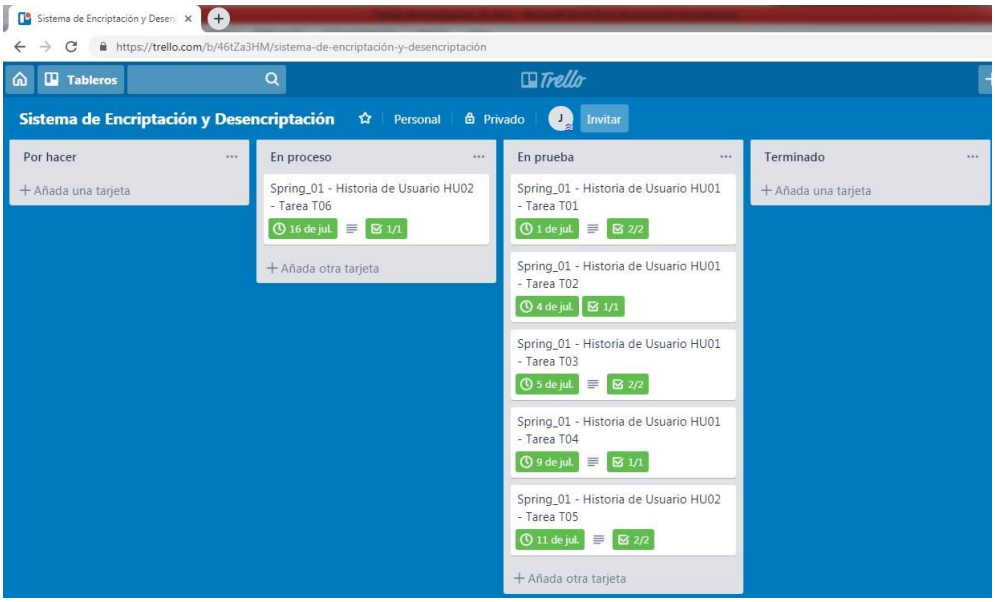


Figura 22. Scrumboard de la tarea T06 en proceso.

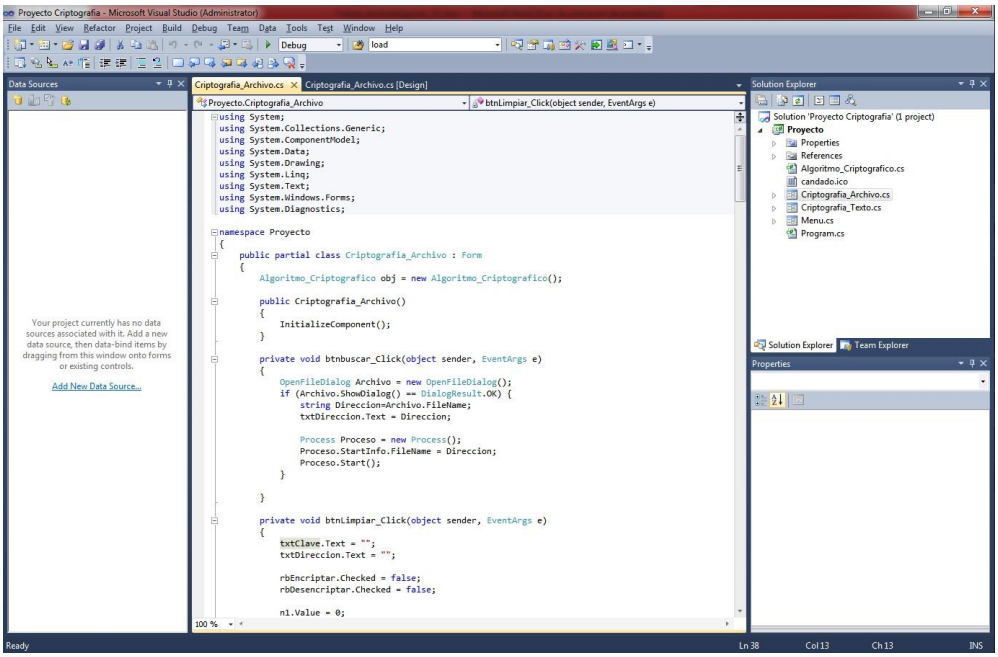


Figura 23. Entregable de la tarea T06

Después del culminar las tareas se realiza el proceso de Prueba o Testing:

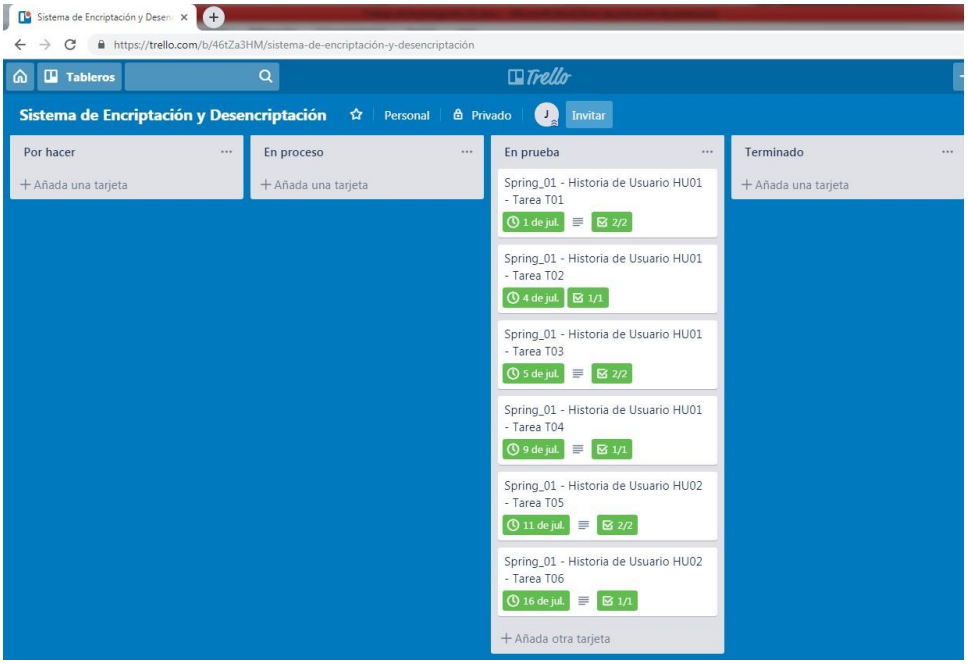


Figura 24. Scrumboard de las tareas en el proceso de prueba.

Resultados del proceso de prueba:

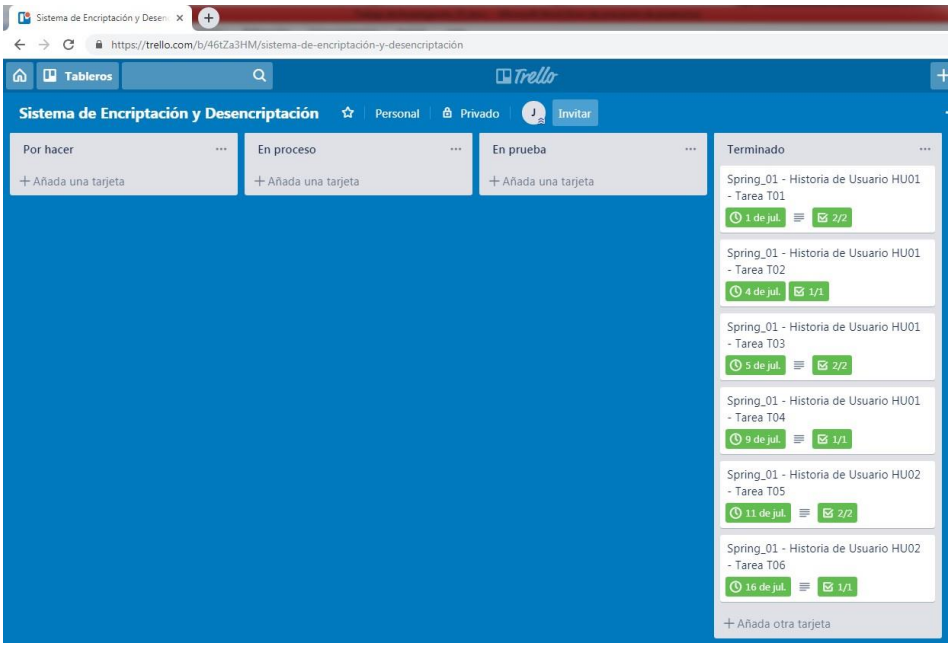


Figura 25. Scrumboard de las tareas terminadas.

Spring	Historia de Usuario	Tarea	Estado Desarrollo	Resultado Testing
Spring 01	HU01	T01	Culminado	Conforme
	HU01	T02	Culminado	Conforme
	HU01	T03	Culminado	Conforme
	HU01	T04	Culminado	Conforme
	HU02	T05	Culminado	Conforme
	HU02	T06	Culminado	Conforme

Tabla 25. Resultado del proceso de Prueba o Testing

Al finalizar el Sprint 01 se recopila la siguiente información del esfuerzo realizado por cada tarea de las Historias de usuario.

Historia de Usuario	Tarea	Tiempo estimado	Tiempo final
HU01	T01	1,66666667	1,5
HU01	T02	10	12
HU01	T03	4,33333333	4
HU01	T04	6,33333333	6
HU02	T05	7,33333333	6
HU02	T06	9	8
Total		**38,6666667**	**37,5**

Tabla 26. Resumen de esfuerzo realizado en el Sprint 01

3.2.2 REVISIÓN Y RETROSPECTIVA

3.2.2.1 DEMOSTRAR Y VALIDAR EL SPRINT

El Equipo SCRUM presenta los entregables al Product Owner y a los Stakeholders del proyecto. A continuación, se presenta un cuadro con los resultados de la evaluación del Sprint 01:

Spring	Historia de Usuario	Tarea	Estado Desarrollo	Resultado Testing	Evaluación
Spring 01	HU01	T01	Culminado	Conforme	Aprobado
	HU01	T02	Culminado	Conforme	Aprobado
	HU01	T03	Culminado	Conforme	Aprobado
	HU01	T04	Culminado	Conforme	Aprobado
	HU02	T05	Culminado	Conforme	Aprobado
	HU02	T06	Culminado	Conforme	Aprobado

Tabla 27. Resultado de evaluación del Sprint 01

3.3 APLICACIÓN

3.3.1 LANZAMIENTO

3.3.1.1 ENVIAR ENTREGABLES

Se hace la presentación de los entregables aceptados por el Product Owner y los Stakeholders, también se programa el pase a producción de acuerdo con la fecha establecida en el proyecto.

Spring	Historia de Usuario	Tarea	Estado Desarrollo	Resultado Testing	Evaluación	Estado
Spring 01	HU01	T01	Culminado	Conforme	Aprobado	Entregado
	HU01	T02	Culminado	Conforme	Aprobado	Entregado
	HU01	T03	Culminado	Conforme	Aprobado	Entregado
	HU01	T04	Culminado	Conforme	Aprobado	Entregado
	HU02	T05	Culminado	Conforme	Aprobado	Entregado
	HU02	T06	Culminado	Conforme	Aprobado	Entregado

Tabla 28. Cuadro de entrega de los entregables del Sprint 01

De acuerdo con el cronograma, el lanzamiento de proyecto es el 16 de julio del 2019.

3.4 MONITOREO

3.4.1 CONTROL DE INCIDENCIAS

En el desarrollo del proyecto de presentó la siguiente incidencia:

- Se tuvo que realizar el cálculo del algoritmo criptográfico de forma manual, siguiendo el método de la regleta, para corroborar que el sistema encriptaba el texto de forma correcta. Por tal motivo tomó más tiempo del indicado el desarrollarlo.

3.5 MANTENIMIENTO

3.5.1 CONTROL DE CAMBIOS

En el desarrollo del proyecto de presentaron los siguientes cambios que no fueron mencionados en las Historias de usuario:

- El sistema, al estar instalado en la PC de la empresa, no se puede utilizar en otros equipos fuera de ella.

  Solución: El sistema será portable, se alojará en un USB y podrá ser utilizado desde cualquier computadora con sistema operativo Windows, desde cualquier lugar sin el uso de internet.
- El archivo txt que contiene el texto a encriptar no debe ser reemplazado por el texto encriptado.

  Solución: Se programó el sistema para que genere un nuevo archivo con el texto encriptado, de esta manera el texto original se mantiene en el archivo original.

CAPITULO IV

ANÁLISIS DE COSTO Y BENEFICIO

4.1 RESULTADOS

Se obtuvieron los siguientes resultados de acuerdo con los objetivos específicos mencionado en el presente documento.

- Objetivo Específico 1: “Analizar y diseñar un sistema que permita encriptar los datos mediante la utilización de herramientas de programación, y el método de cifrado de la Regleta.”

  Se utilizó un método seguro para el cifrado, el método de la regleta, y se tuvo como resultado un sistema diseñado a la medida, de acuerdo con los requerimientos de la empresa. A su vez es fácil de usar, amigable para el usuario y es portable.

- Objetivo Específico 2: “Implementar el sistema como herramienta de soporte en la empresa Deutsche Pharma.”

  Se tuvo como resultado una herramienta muy útil para la seguridad de la información. También se redujo el nivel de riesgo que había, al tener la información compartida en la red, en un 10%. El sistema solo podrá ser usado en un sistema operativo Windows.

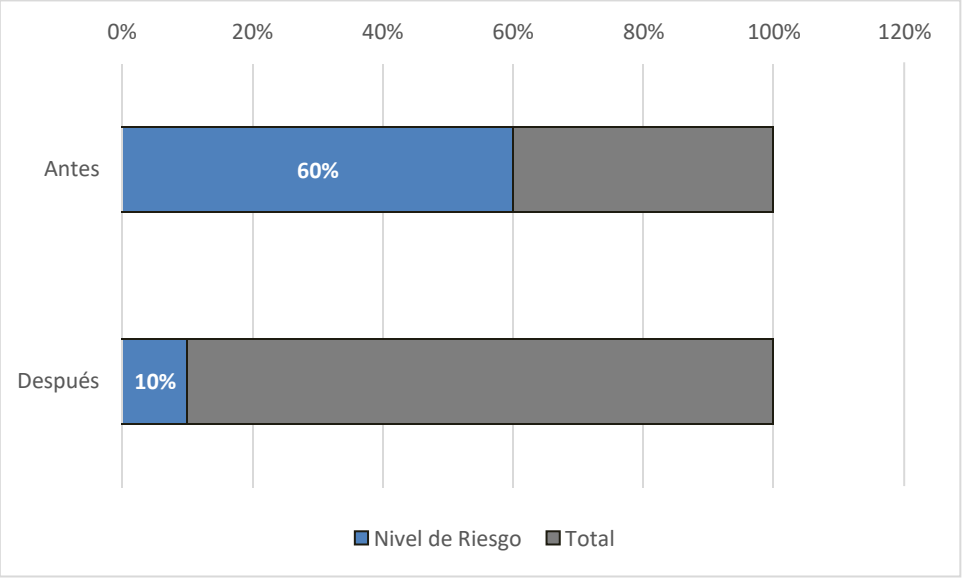


Figura 26. Gráfico de comparación de riesgos antes y después de la implementación

4.2 ANALISIS DE COSTOS

4.2.1 COSTO DE PERSONAL

Las personas, que conforman al equipo SCRUM, involucradas en el presente proyecto son: el Jefe de proyecto (SCRUM Master), el Analista programador y el QA Tester. En el siguiente cuadro se están considerando las horas del tiempo del desarrollo del proyecto, así como el trabajo en horas de cada miembro del equipo.

Personal	Cantidad	Horas	Costo x Hora(S/)	Costo(S/)
Jefe de Proyecto	1	20	70,00	1.400,00
Analista Programador	1	37,5	35,00	1.312,50
QA Tester	1	8	30,00	240,00
			COSTO TOTAL	**2.952,50**

Tabla 29. Costo de personal

4.2.2 COSTO DE TECNOLOGÍA

Los costos en tecnología son hardware y software. Como hardware se solicitó una laptop con 8GB de RAM y una capacidad de disco duro de 1 TB. También se requirió el

programa Visual Studio 2013 con licencia, además de la herramienta online Trello que es de uso gratuito. En el siguiente cuadro se detalla el costo de cada tecnología.

Tecnología	Cantidad	Costo(S/)
HP LAPTOP 15-DA0028LA 15.6" CORE I5 1TB 8GB	1	2.399,00
Visual Studio 2013	1	8.734,60
Trello	1	-
	COSTO TOTAL	**11.133,60**

Tabla 30. Costo de Tecnología

4.2.3 COSTOS TOTALES

Para este proyecto los costos totales, considerando los costos de personal y los costos de tecnología, fueron:

- Personal: **2.952,50**
- Tecnología: **11.133,60**

Por lo tanto, el coto total invertido en el proyecto es de **S/ 14.086,10**.

4.3 ANALISIS DE BENEFICIOS

El proyecto elaborado presenta solo beneficios cualitativos. Se considera que los problemas específicos y generales fueron solucionados. Como resultado se tiene lo siguiente:

- Se analizó la posibilidad de diseñar un sistema de escritorio para la empresa. A su vez se encontró un método de cifrado seguro para fortalecer el algoritmo criptográfico. Se identificaron los requerimientos, conocidos también como Historias de usuario, los cuales sirvieron para hacer un sistema a medida.

- La implementación del sistema criptográfico pasó con éxito a producción,

cumpliendo de esa manera el objetivo general de analizar, diseñar e implementar un sistema de escritorio que permita encriptar la información que se comparte en la red; teniendo así una herramienta de soporte en seguridad.

CONCLUSIONES

- Se realizó el análisis, diseño e implementación del sistema de encriptación de datos de manera exitosa. Con un cifrado seguro y con un diseño amigable para el usuario.

- El proyecto se pudo desarrollar de forma rápida gracias a la metodología SCRUM, ya que se distribuyó el proyecto en tareas que se podían monitorear en el proceso del cumplimiento de estas. Se redujeron los errores ya que se validaba cada entregable antes del pase a producción.

- Debido a que se implementó un sistema de encriptación de datos se redujeron los riesgos de la vulnerabilidad de la información en un 10%. Permitiendo tener la información en la red de una manera segura.

- Se identificó que para poder trabajar con una metodología ágil es necesario utilizar una herramienta de gestión de proyectos, que permita realizar un seguimiento en el desarrollo y cumplimiento de las tareas, para así presentar los entregables en el tiempo indicado.

RECOMENDACIONES

- Se recomienda tener conocimiento del método de la regleta, acerca de su funcionamiento y las posibles formas de utilizarlo, con el fin realizar el algoritmo criptográfico de forma correcta y con más niveles de seguridad.

- Es necesario que el equipo SCRUM se reúna después del término de cada entregable, para así poder identificar las posibles mejoras dentro del tiempo establecido de los entregables. De esta manera se cumplirán con los tiempos del proyecto y con mejores resultados.

- El sistema solo podrá ser utilizado en un sistema operativo Windows. Se recomienda implementar una nueva versión que pueda utilizarse desde cualquier sistema operativo.

BIBLIOGRAFÍA

Chaves Jiménez, H. (2008). Diseño e implementación de un software multimediapara el aprendizaje de la Criptografía. *Diseño e implementación de un software multimediapara el aprendizaje de la Criptografía*. Bogotá.

Fernández, J., & Cadelli, S. (2014). Convivencia de metodologías: Scrum y Rup en un proyecto de gran escala. *Convivencia de metodologías: Scrum y Rup en un proyecto de gran escala*.

Gestron. (01 de Julio de 2019). Obtenido de Gestron: http://gestron.es/que-es-trello/#Que_es_Trello

Granados, G. (10 de Julio de 2006). Introducción a la Criptografía. *Revista Diginal Universitaria, 7*(7), 2-8. Obtenido de https://profecd.webnode.es/_files/200000079-90fc291f71/Introduccion%20a%20la%20criptografia.pdf

Internet ya. (07 de Febrero de 2018). Obtenido de Internet ya: https://www.internetya.co/aplicaciones-web-vs-escritorio/

Real Academia Española. (s.f.). Obtenido de Real Academia Española: http://www.rae.es/

Rodríguez Marín, L. (s.f.). Criptografía. *Criptografía - Departamento de Matemática Aplicada UNED*. Obtenido de http://portal.uned.es/pls/portal/docs/PAGE/UNED_MAIN/LAUNIVERSIDAD/UBICACIONES/08/DOCENTE/LUIS_FEDERICO_RODRIGUEZ_MARIN/MATEMATICA%20RECREATIVA/CRIPTOGRAF%C3%8DA.%20ACTIVIDADES%20CON%20CIFRARIOS%20Y%20REJILLAS%20.PDF

Rodriguez, V. (20 de Junio de 2016). *Acerca de nosotros: Segurisoft*. Recuperado el 26 de Setiembre de 2018, de sitio web de Segurisoft: https://www.segurisoft.es/encriptacion/top-10-software-encriptacion/

Rosado, S. (07 de Febrero de 2019). *Tabla comparativa de los lenguajes de programación*. Obtenido de Tabla comparativa de los lenguajes de programación:

http://desarrollowebydesarrolloweb.blogspot.com/2015/02/tabla-comparativa-de-loslenguajes-de.html

Satpathy, T. (2017). *Una guía para el CUERPO DE CONOCIMIENTO DE SCRUM (Guía SBOK™)* (Tercera Edición ed.). Avondale, Arizona, USA: SCRUMstudy™.

Schwaber, K., & Sutherland, J. (Julio de 2016). La Guía de Scrum TM. En K. Schwaber, & J. Sutherland, *La Guía de Scrum TM* (págs. 3-17).

ANEXO 1

GLOSARIO

Criptografía: Es una ciencia que se encarga de proteger los datos disfrazándolos con códigos o cifras para mantenerlos en secreto.

Metodología: Consiste en un conjunto de métodos que son aplicados en un proceso de investigación científica.

SCRUM: Es una metodología, conocida como ágil, contiene un conjunto de buenas prácticas para la gestión de proyectos.

RUP: Es una metodología estándar, utilizada generalmente para la gestión de proyectos de desarrollo de software.

Portable: Es un sistema o aplicación que pude ser utilizado sin la necesidad de ser instalado en una computadora. Solo funciona con el sistema operativo para el que fue creado.

Cifrado: Es un texto que está escrito con diferentes caracteres, solo podrá ser traducido si se posee una clave para descifrar el texto.

Software: Es un programa que contiene un conjunto de datos y procedimientos para realizar tareas que le fueron programadas en una computadora.

Lenguaje de programación: Es una serie de códigos con una estructura determinada que son entendidos por un sistema de programación.

Licencia: Consiste en un contrato donde se autoriza el uso de un software, cumpliendo con los términos y condiciones establecidos.

Scrumboard: Es una herramienta de SCRUM, consiste en un tablero o pizarra donde se representa el estado de las tareas del proyecto.

Sprint: En SCRUM es un ciclo o iteración de un proyecto. Su duración es entre dos y cuatros semanas.

Product Owner: En SCRUM es un actor importante del proyecto, ya que es el encargado de la comunicación entre el equipo SCRUM y terceros.

Stakeholders: Son todas las personas interesadas y que se ven afectadas en el desarrollo de un proyecto en una empresa.

Algoritmo: Es un conjunto de pasos u operaciones ordenas de manera lógica, que dan un resultado.

ANEXO 2

MANUAL DE USUARIO

El usuario deberá ingresar al sistema, el sistema mostrará una ventada con dos opciones:

1. Texto: El usuario podrá encriptar y desencriptar un texto por medio de una palabra clave y un número clave.
2. Archivo: El usuario podrá encriptar y desencriptar un texto que se encuentra en un archivo con extensión .txt por medio de una palabra clave y un número clave.

1. Texto:

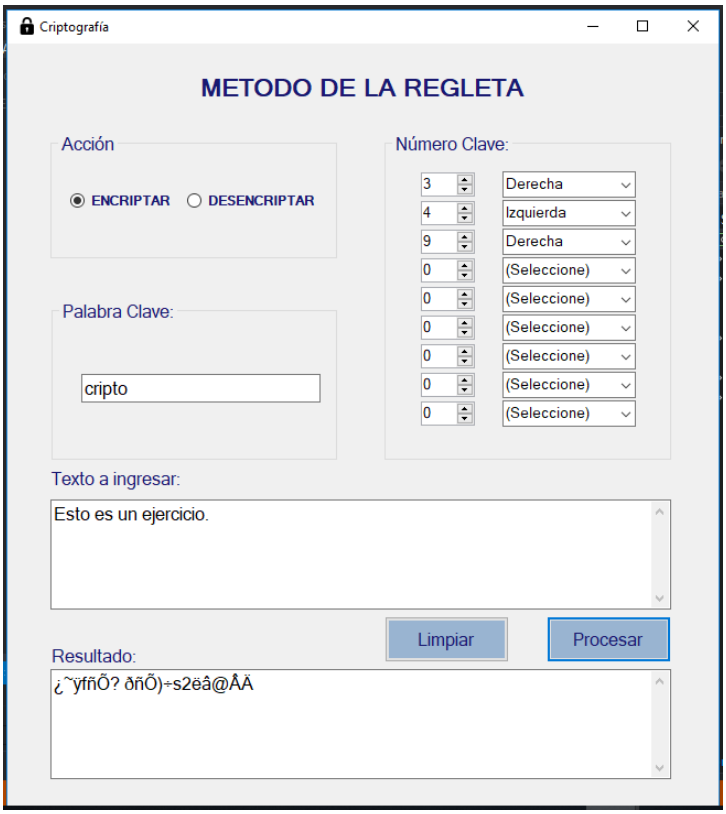
El sistema mostrará una ventana donde el usuario podrá encriptar y desencriptar un texto ingresado. Sus elementos son:

- Acción:
    - Encriptar: El sistema generará el texto cifrado.
    - Desencriptar: El sistema convertirá el texto cifrado a su lenguaje

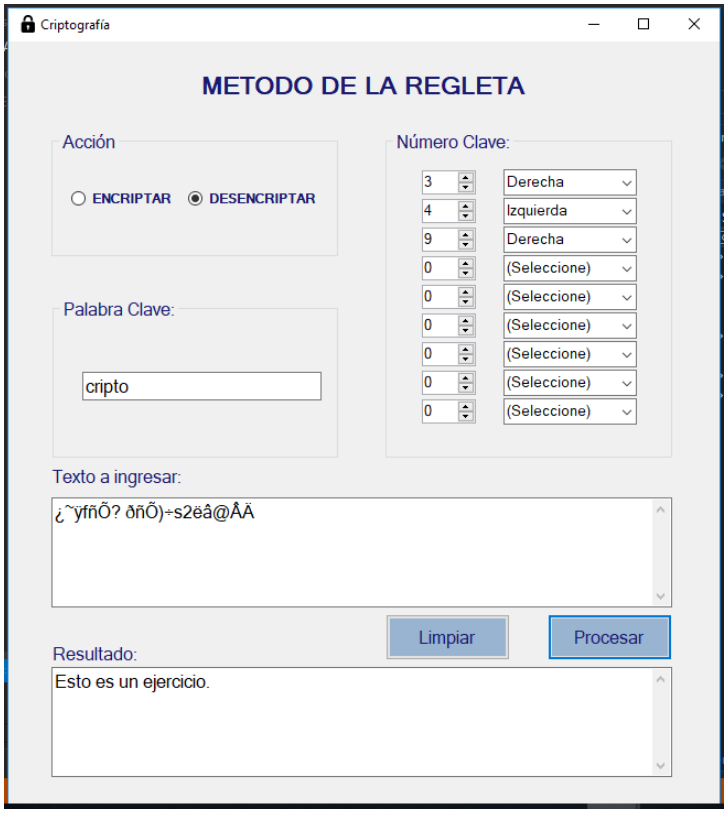
original.

- Número Clave: El usuario podrá ingresar una clave numérica de hasta 9 dígitos e indicar su dirección de recorrido en el algoritmo de la Regleta (Derecha, izquierda o normal), servirá para encriptar y desencriptar el texto ingresado.
- Palabra clave: El usuario ingresará una palabra clave, la cual servirá para encriptar y desencriptar el texto ingresado.
- Texto por ingresar: Caja de texto donde el usuario podrá ingresar el texto a encriptar.
- Limpiar: Botón con el cual el usuario borrará los criterios ingresados.
- Procesar: Botón con el cual el usuario ejecutará la encriptación o desencriptación del texto ingresado.
- Resultad: Caja de texto donde se mostrará el resultado de la encriptación o desencriptación.

Resultado de la encriptación del texto ingresado:



Resultado de la desencriptación del texto ingresado:



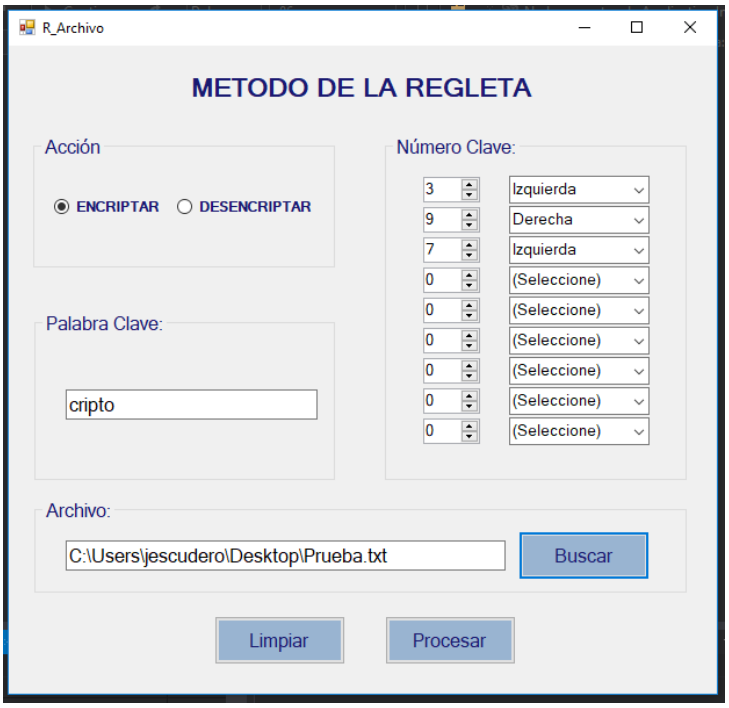
2. Archivo:

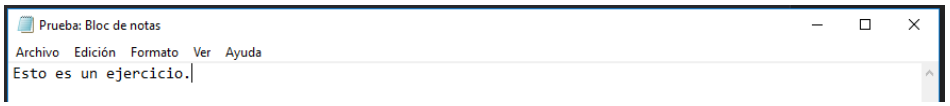
El sistema mostrará una ventana donde el usuario podrá encriptar y desencriptar el texto existente de un archivo seleccionado. Sus elementos son:

- Acción:
    - Encriptar: El sistema generará el texto cifrado.
    - Desencriptar: El sistema convertirá el texto cifrado a su lenguaje original.
- Número Clave: El usuario podrá ingresar una clave numérica de hasta 9 dígitos e indicar su dirección de recorrido en el algoritmo de la Regleta (Derecha, izquierda o normal), servirá para encriptar y desencriptar el texto ingresado.
- Palabra clave: El usuario ingresará una palabra clave, la cual servirá para encriptar y desencriptar el texto ingresado.
- Archivo: Caja de texto que mostrará la ruta del archivo seleccionado.
- Buscar: Botón con el cual el usuario entrará al explorador de archivos y seleccionará el archivo que contiene el texto a encriptar.
- Limpiar: Botón con el cual el usuario borrará los criterios ingresados.
- Procesar: Botón con el cual el usuario ejecutará la encriptación o desencriptación del texto que se encuentra en el archivo seleccionado. El sistema mostrará el contenido del archivo con el texto encriptado o desencriptado.

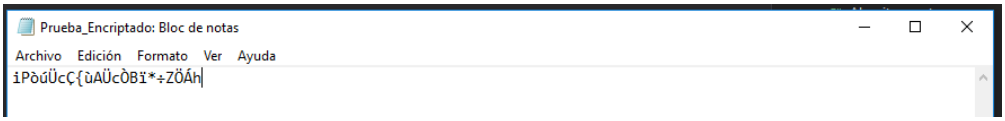
Resultado de la encriptación del texto del archivo seleccionado:

- Antes de procesar:



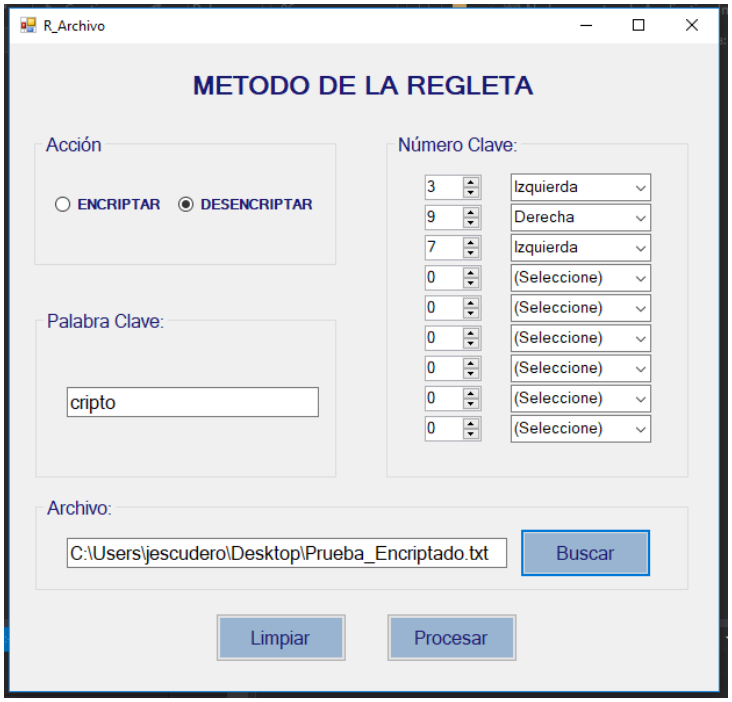


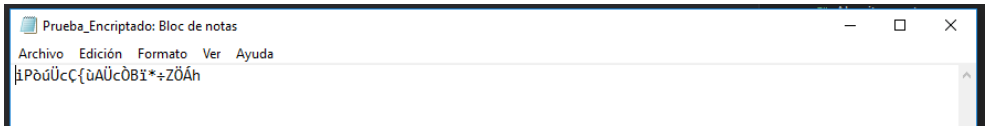
- Después de procesar:



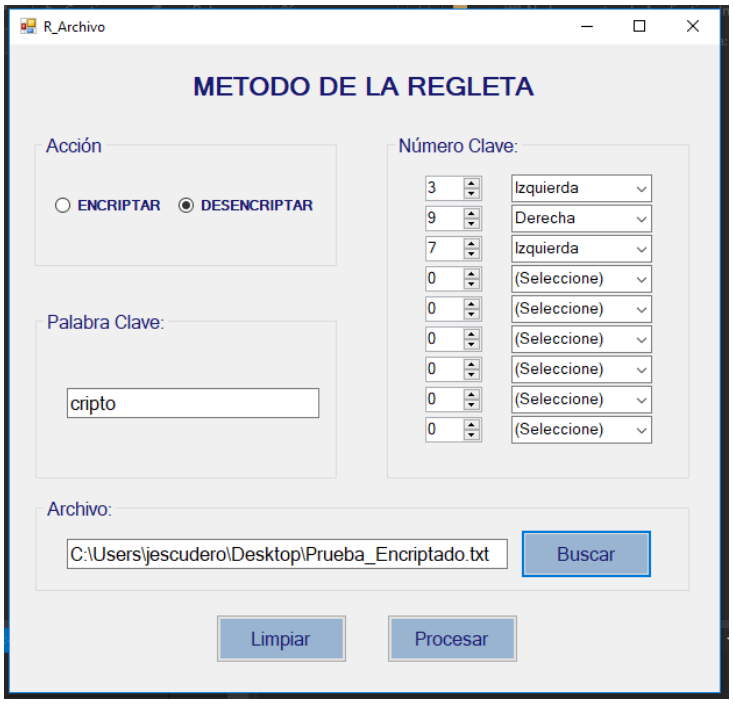
Resultado de la desencriptación del texto del archivo seleccionado:

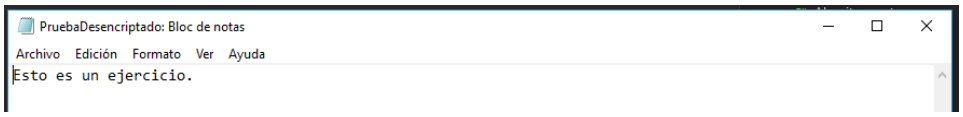
- Antes de procesar:





- Después de procesar:


R_Archivo
METODO DE LA REGLETA
Acción
ENCRIPTAR
DESENCRIPTAR
Palabra Clave:
cripto
Número Clave:
3 Izquierda
9 Derecha
7 Izquierda
0 (Seleccione)
0 (Seleccione)
0 (Seleccione)
0 (Seleccione)
0 (Seleccione)
0 (Seleccione)
Archivo:
C:\Users\jescudero\Desktop\Prueba_Encriptado.txt
Buscar
Limpiar
Procesar


PruebaDesencriptado: Bloc de notas
Archivo Edición Formato Ver Ayuda
Esto es un ejercicio.